NetCommWireless

User **Guide**

NWL-15 – Light Industrial M2M Router Plus

Copyright

Copyright© 2014 NetComm Wireless Limited. All rights reserved.

The information contained herein is proprietary to NetComm Wireless. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Wireless.

Note: This document is subject to change without notice.

Save our environment

When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separately from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this device can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

This guide covers the following products:

NetComm Wireless NWL-15-02 Light Industrial M2M Router Plus

DOCUMENT VERSION	DATE
1.0 - Initial document release	May 22, 2014

Table 1 - Document Revision History

NetCommWireless

Table of contents

Overview 5
Introduction 5
Target audience 5
Prerequisites 5
Notation 5
Product introduction 6
Product overview 6
Package contents 6
Product features 7
Physical dimensions and indicators 8
Physical dimensions 8
LED indicators 9
Ethernet port LED indicators 10
Interfaces 11
Placement of the router 12
Mounting options 12
Powering the router 17
Power consumption 18
Installation and activation of the NWL-15 router 19
Installing the router 19
Activating the router 20
Advanced configuration 21
Status 21
Networking 23
Data connection 23
Connect on demand 28
Operator settings 32
LAN 33
Routing 37
VPN 47
Services 60
Dynamic DNS 60
Network time (NTP) 61
Data stream manager 62
Legacy data managers 67
Watchdogs 70
SNMP 73
TR-069 75
GPS 77
Odometer 79
IO configuration 80
Low power mode 82
SMS 86
Diagnostics 90
Sending an SMS diagnostic command 93
System 100
Log 100
System configuration 103
HTTPS Key Management 110
SSH key management 113
Appendix A: Tables 117
Appendix B: Device mounting dimensions 118
Appendix C: Mounting bracket 119
Appendix D: Default settings 120
Restoring factory default settings 121
Appendix E: Recovery mode 122
Accessing recovery mode 122
Status 123
Log 123
Application installer 124
Settings 124
Reboot 124
Appendix F: HTTPS - Uploading a self-signed certificate 125
Appendix G: RJ-45 connector 127
Appendix H: Serial port wiring 128
Appendix I: Inputs/Outputs 129
Overview 129

Technical data 134
Safety and product care 135
Product warranty 139

Overview

Introduction

This document provides you all the information you need to set up, configure and use the NetComm Wireless NWL-15 router.

Target audience

This document is intended for system integrators or experienced hardware installers who understand telecommunications terminology and concepts.

Prerequisites

Before continuing with the installation of your NWL-15 router, please confirm that you have the following:

- A device with a working Ethernet network adapter.
- A web browser such as Internet Explorer, Mozilla Firefox or Google Chrome.
- A flathead screwdriver if field terminated power is required.

Notation

The following symbols are used in this user guide:

The following note requires attention.

The following note provides a warning.

The following note provides useful information.

Product introduction

Product overview

- Dual-band CDMA (BC0/BC1), 800/1900MHz
- CDMA data speeds up to 3.1 Mbps DL
- RS232/RS422/RS485 Port and USB 2.0 OTG port
- Built in GPS supporting an active GPS Antenna via external SMA connector
- Three multi-purpose I/O ports
- One dedicated ignition input
- Intelligent, Tri-Colour LED display for clear, easy to read modem status information
- Extensive device management with support for TR-069, Web GUI and full feature management with SMS
- Optimized web configuration UI
- Flexible mounting suitable for in-home use or industrial applications with built-in wall mount, and DIN rail mounting options

Package contents

The NetComm Wireless NWL-15 router package consists of:

- 1 x NWL-15 router
- 1 x Six-way terminal block
- 1 x 1.5m yellow Ethernet cable 8P8C
- 2 x CDMA antennas
- 1 x DIN rail mounting bracket
- 1 x Quick start guide

If any of these items are missing or damaged, please contact NetComm Wireless Support immediately. The NetComm Wireless Support website can be found at: http://support.netcommwireless.com.

Product features

The NWL-15 router is a high performing dual band CDMA Router that delivers the high speed and wide coverage afforded by Verizon's CDMA network. Designed for plug and play Ethernet IP connectivity, its lightweight, compact design makes it suitable for a broad range of industry applications. The device incorporates state-of-the-art M2M features; a powerful external antenna with an additional antenna providing diversity assistance; flexible mounting options and a wide operating temperature range. The device enables you to remotely connect your assets, premises or equipment to gather real-time business insight and streamline your business operations. The router's open Linux operating system and Software Development Kit (SDK) offers the capability to install custom software applications within the substantial onboard flash memory. The device also allows remote system monitoring, remote diagnostics, remote configuration and firmware updates over the air. Featuring Ethernet, Serial (RS232/422/485), and USB 2.0 connectivity, the NWL-15 router can interface with a diverse range of equipment used in a wide variety of vertical applications. The NWL-15 router also features built in GPS support and a dedicated ignition input making it ideal for vehicle applications. The device features multipurpose digital and analogue I/O ports and is compatible with the NetComm Wireless Software Development Kit allowing you to customize their functionality to your needs.

Physical dimensions and indicators

Physical dimensions

Below is a list of the physical dimensions of the NWL-15 router.

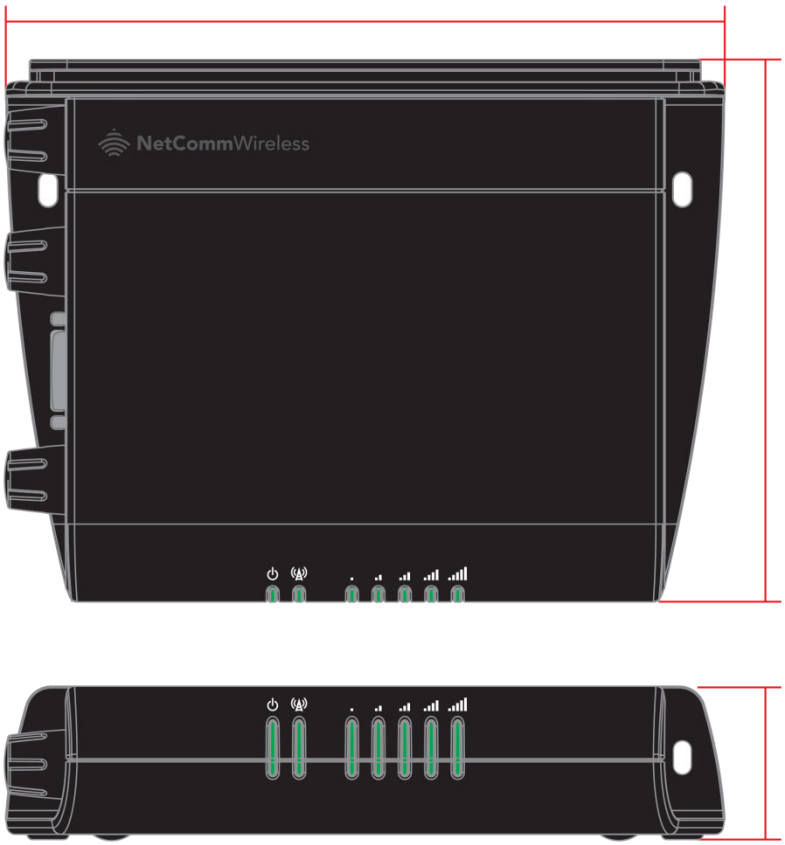


Figure 1 – NWL-15 dimensions

NWL-15 ROUTER (WITHOUT EXTERNAL ANTENNA ATTACHED)	
Length	140 mm
Depth	103 mm
Height	30 mm
Weight	180g

Table 2 - Device Dimensions

LED indicators

The NWL-15 router uses 7 LEDs to display the current system and connection status.

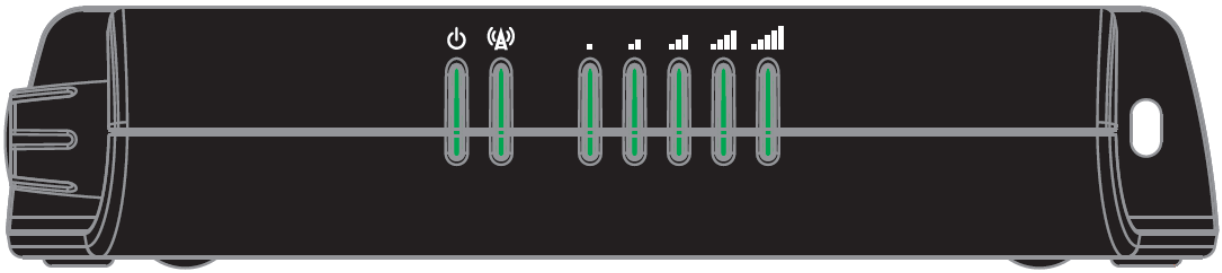


Figure 2 - NWL-15 router LED Indicators

LED ICON	NAME	COLOR	STATE	DESCRIPTION
	Power		Off	Power off
			Double flash	Powering up
			On	Power on
			On	Power on in recovery mode
			Slow flashing	Hardware error
	Network		On	Connected via WWAN
			Blinking[1]	Traffic via WWAN
			Slow flashing	Connecting data session
			On	Registered network
			Slow flashing	Registering network
			On	Can't connect
			Slow flashing	Not activated
	Signal strength		On	EVDO coverage
			On	CDMA 1x coverage

Table 3 - LED Indicators

[1] The term "blinking" means that the LED may pulse, with the intervals that the LED is on and off not being equal. The term "flashing" means that the LED turns on and off at equal intervals.

Signal strength LEDs

The following table lists the signal strength range corresponding with the number of lit signal strength LEDs.

NUMBER OF LIT LEDS	SIGNAL STRENGTH
All LEDs unlit	< -109 dBm
1	-109 dBm to -102dBm
2	-101 dBm to -92 dBm
3	-91 dBm to -86 dBm
4	-85 dBm to -78 dBm
5	≥ -77 dBm

Table 4 - Signal strength LED descriptions

LED update interval

The signal strength LEDs update within a few seconds with a rolling average signal strength reading. When selecting a location for the router or positioning an external antenna, please allow up to 20 seconds for the signal strength LEDs to update before repositioning.

Ethernet port LED indicators

The Ethernet port of the NWL-15 router has two LED indicators on it.

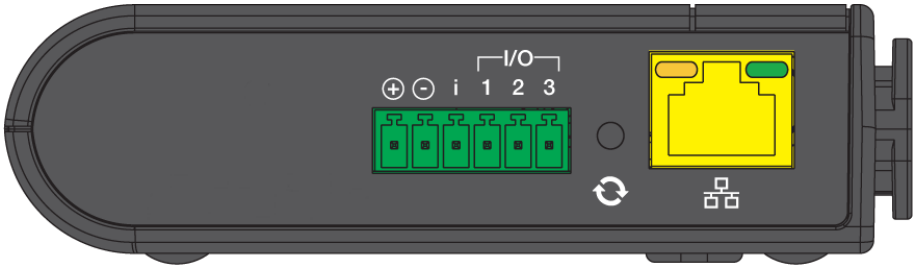


Figure 3 - Ethernet port LED indicators

The table below describes the statuses of each light and their meanings.

LED	STATUS	DESCRIPTION
Green	On	There is a valid network link.
	Blinking	There is activity on the network link.
	Off	No valid network link detected.
Amber	On	The Ethernet port is operating at a speed of 100Mbps.
	Off	The Ethernet port is operating at a speed of 10Mbps or no Ethernet cable is connected.

Table 5 - Ethernet port LED indicators description

Interfaces

The following interfaces are available on the NWL-15 router:

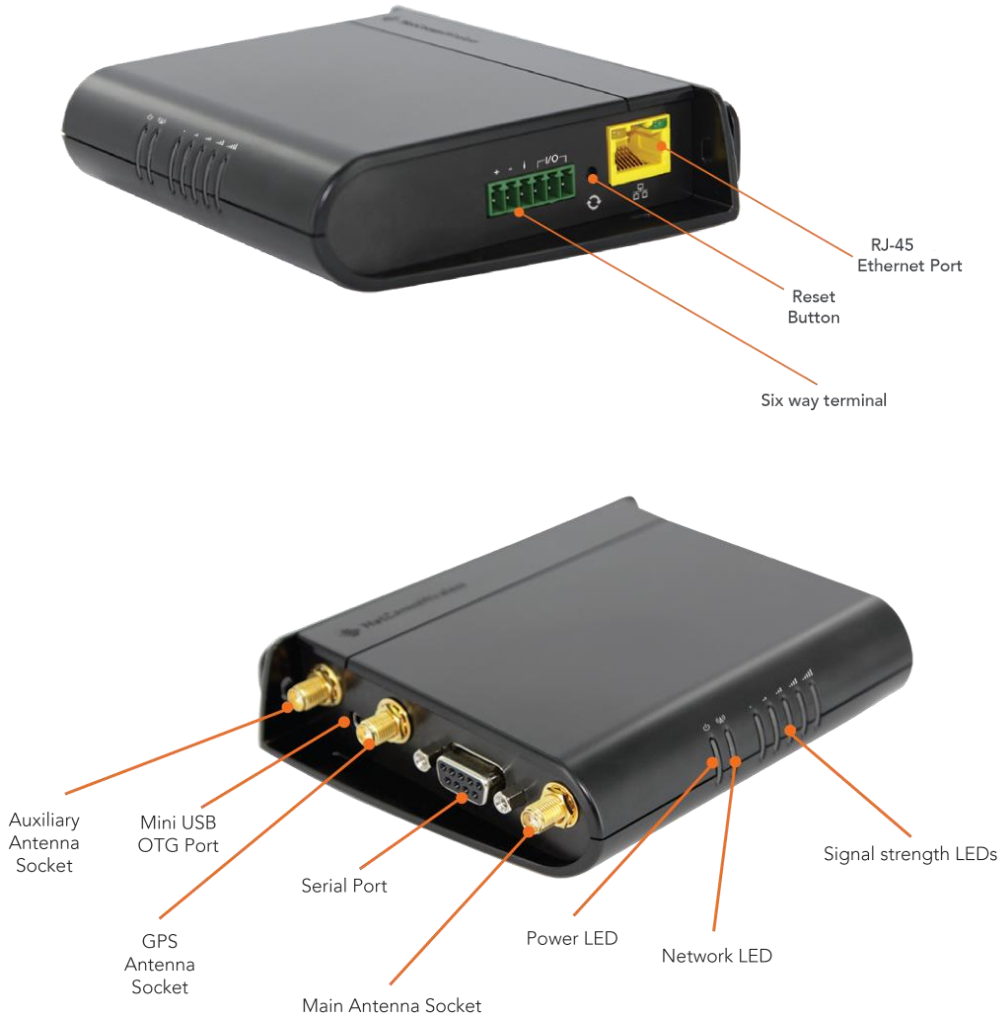


Figure 4 - Interfaces

ITEM	DESCRIPTION
RJ45 Ethernet port	Connect one or several devices via a network switch here.
Reset button	Press and hold for less than 5 seconds to reboot to normal mode. Press and hold for 5 to 15 seconds to reboot to recovery mode. Press and hold for 15 to 20 seconds to reset the router to factory default settings.
Six-way terminal	Connect power source, ignition and I/O wires here. Power, ignition and I/O wires may be terminated on the supplied terminal block and connected to a power source. Refer to the diagram and table under the Powering the router section for correct wiring of the terminal block. Operates in the 8-40V DC range.
Main antenna socket	SMA female connector for main antenna.
Auxiliary antenna socket	SMA female connector for auxiliary antenna (receive diversity).
Mini USB 2.0 OTG port	Provides connectivity for optional external storage or a USB Ethernet dongle. Supplies up to 0.5A to connected device.
Serial port	Female DB9 port supporting 9-wire RS-232, RS-485 or RS-422 (software selectable).
GPS antenna socket	SMA female connector for an active GPS antenna.

Table 6 – Interfaces

Placement of the router

The two external high-performance antennas supplied with the router are designed to provide optimum signal strength in a wide range of environments. If you find the signal strength is weak, try adjusting the orientation of the antennas. If you are unable to get an acceptable signal, try moving the router to a different place or mounting it differently.

Note: When selecting a location for the router, allow at least 20 seconds for the signal strength LEDs to update before trying a different location or connecting an external antenna.

Mounting options

The NWL-15 router can be quickly and easily mounted in a variety of locations.

Mounted flat against the wall

When mounted flat against the wall, the NWL-15 router has a slimline form factor. Use appropriately sized screws in the mounting holes provided on the base of the unit.

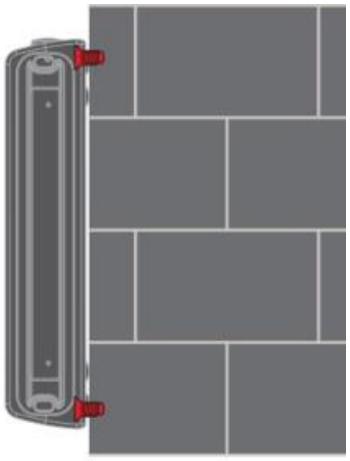


Figure 5 - Wall mount - Flat against the wall

Perpendicular to the wall

If a large surface area is not available, there is the option of mounting the router perpendicular to the wall. This gives the router a small wall footprint while remaining securely attached. Use appropriately sized screws in the mounting holes provided on the back of the unit.

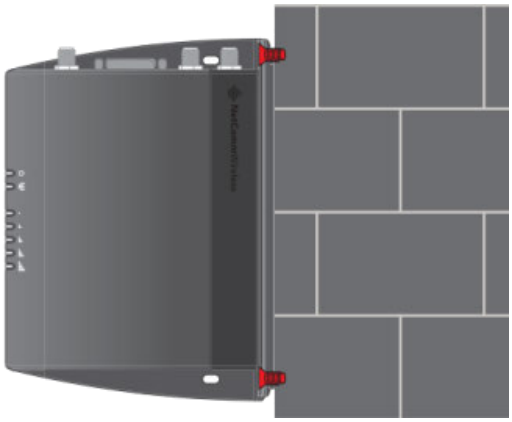


Figure 6 - Wall mount - Perpendicular to the wall

C Section DIN Rail mount

The NWL-15 router easily slides onto a C Section DIN rail so that it is horizontally mounted. The DIN Rail mounting bracket is not required for C Section DIN rail mounting.

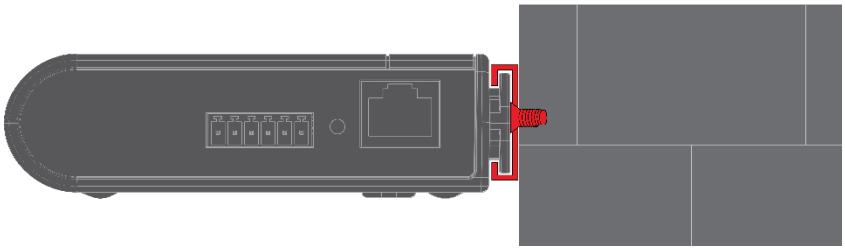


Figure 7 - C Section DIN rail mount

To mount the unit on a C-Section DIN rail, slide it on as illustrated below:

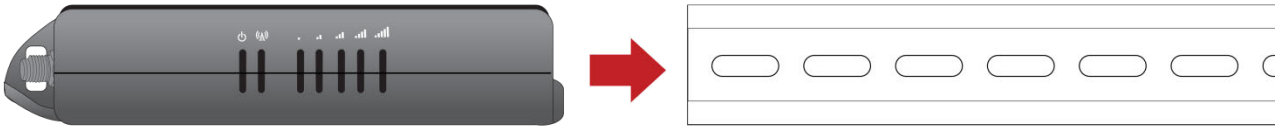


Figure 8 - Mounting the unit on a DIN rail

Mounting bracket

The provided mounting bracket provides additional methods of mounting the NWL-15 router.

To attach the mounting bracket, slide it onto the rear of the router as shown in the diagram below:

Figure 9 - Sliding on the mounting bracket

To remove the bracket, press the PUSH button and slide the router off the bracket:

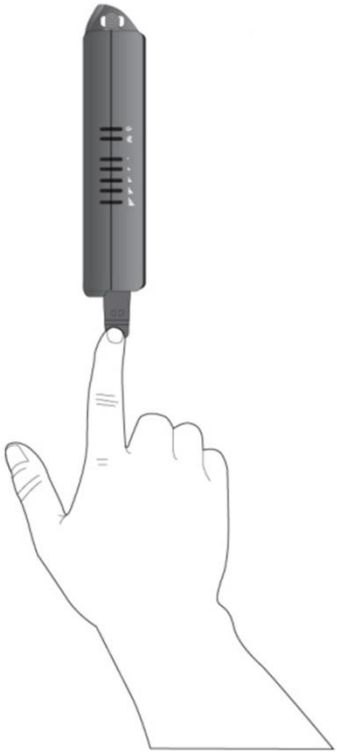


Figure 10 - Removing the mounting bracket

Using the mounting bracket for wall mounting

By first attaching the DIN rail bracket to the wall, the NWL-15 router can be easily attached and removed from the bracket.

Figure 11 – Wall mount - Mounted via DIN rail bracket

Using the mounting bracket for Top hat DIN rail mounting

The NWL-15 router may be vertically mounted to the wall with the bracket by sliding the bracket onto a top hat DIN rail

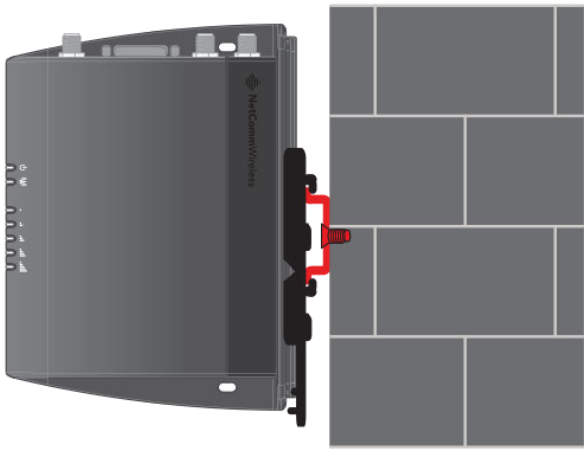


Figure 12 - Top hat DIN rail mount

Alternatively, you can attach it to the DIN Rail by using the V bend in the bracket as illustrated below:

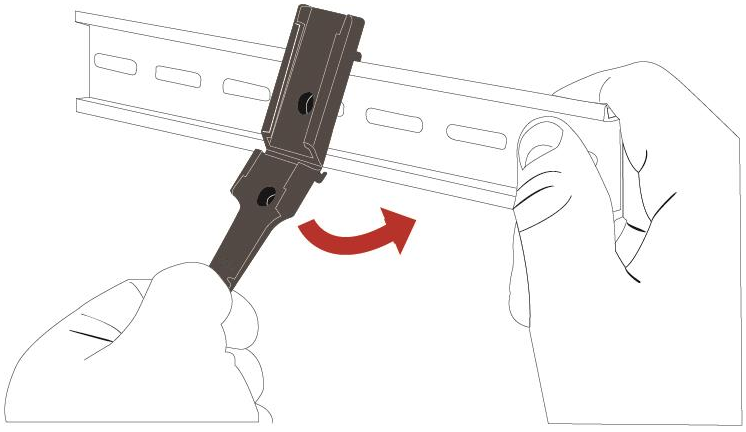


Figure 13 - Attaching the mounting bracket to the DIN rail using the V bend

Desk mount

In situations where wall mounts and DIN rails are not required, you can simply place the NWL-15 router on a desk using its rubber feet to prevent it from slipping.

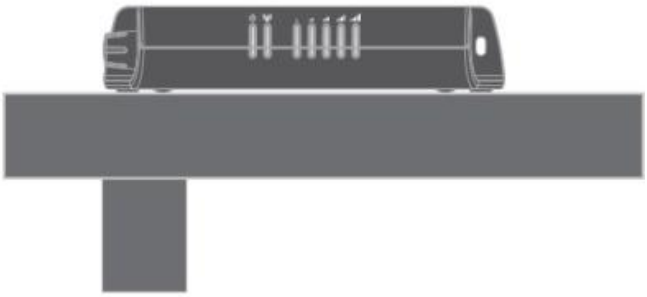


Figure 14 - Desk mount

Powering the router

The NWL-15 router can be powered in one of two ways:

1. DC power input via 6-pin connector (8-40V DC)
2. DC power input via field terminated power source (8-40V DC)

The green power LED on the router lights up when a power source is connected.

DC power via 6-pin connector

The DC input jack can accept power from a separately sold DC power supply. Both a standard temperature range DC power supply and an extended temperature range DC power supply are available to purchase as accessories.

To power the device via DC Power via the 6-pin connector, remove the attached green terminal block from your router and connect the external DC power supply to the router's green DC power jack.

DC power via field terminated power source

If an existing 8-40V DC power supply is available, you can insert the wires into the supplied terminal block to power your router. Use a flathead screwdriver to tighten the terminal block screws and secure the power wires, making sure the polarity of the wires are correctly matched, as illustrated below.

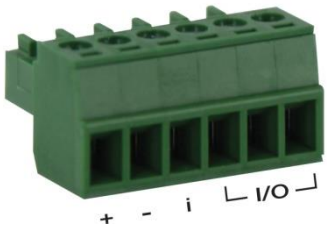


Figure 15 - Locking Power Terminal Block

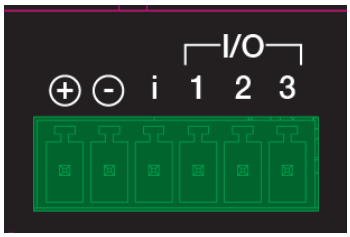


Figure 16 – Terminal block connector

TERMINAL	DESCRIPTION
+	Positive wire for power.
-	Ground wire.
i	Dedicated terminal for ignition detection.
I/O	Three terminals used for input/output detection (refer to the IO configuration section for more information).

Table 7 - Locking power block pin outs

Viewing power source information

You can view the current power input mode in the **Advanced status** section of the device's web user interface. This is useful for remotely monitoring the device. You can also use the Software Development Kit to access this information for advanced purposes (e.g. configuring SMS alerts to inform you of the power status of the router).

To view the router's power source information, log in to the router and expand the **Advanced status** box on the status page. See the Status section of this manual for more information on the status page.

Power consumption

To assist with power consumption planning, the following table summarizes average power consumption during the various states of the NWL-15 router under normal usage conditions. It's important to note that this table serves as an indication only as the power consumed by the device is affected by many variables including signal strength, network type, and network activity.

Average power consumption figures

STATE	POWER CONSUMPTION
Powered on, idle and connected to packet data	1.2W
Powered on, connected to packet data with average load	2.0W
Powered on, connected to packet data with heavy traffic	4.0W
Peak power draw at maximum 3G module transmission power	5.0W

Table 8 - Average power consumption figures

Installation and activation of the NWL-15 router

Installing the router

After you have mounted the router and connected a power source, follow these steps to complete the installation process.

1. Connect equipment that requires network access to the Ethernet port of your router. This may be your computer for advanced configuration purposes, or your end equipment which requires data access via the NWL-15 router. You can connect one device directly, or several devices using a network switch.
2. Ensure the external power source is switched on and wait 2 minutes for your NWL-15 router to start up. To check the status of your router, compare the LED indicators on the device with those listed on page 8 of this guide.
3. Open a web browser (e.g. Internet Explorer, Firefox, Safari), type http://192.168.1.1 into the address bar and press **Enter**. The web-based user interface log in screen is displayed.

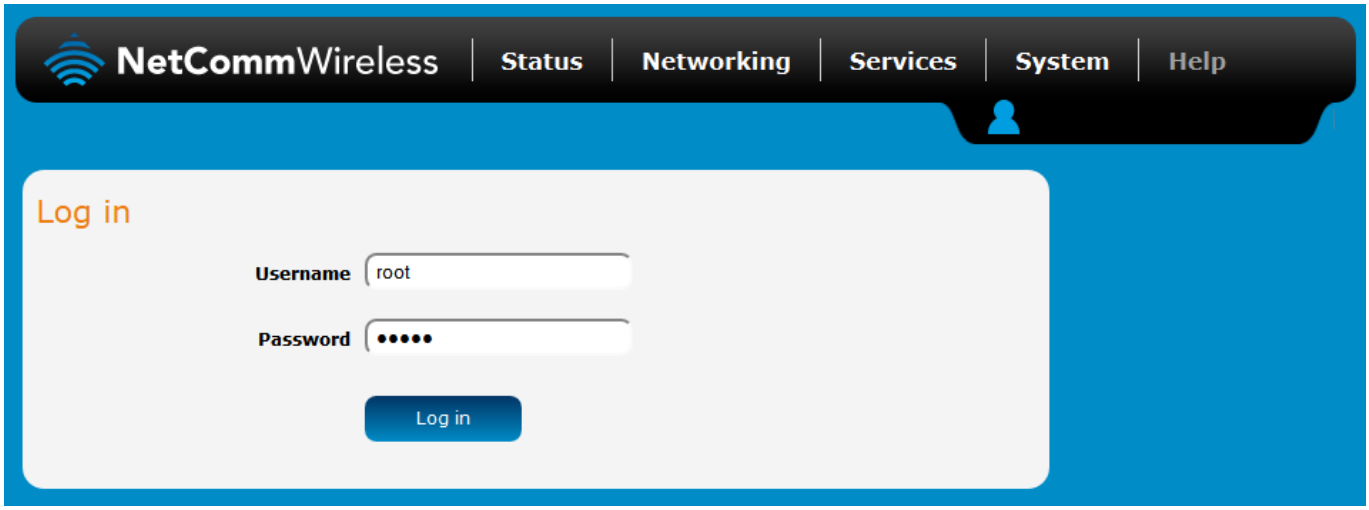


Figure 17 – Log in prompt for the web-based user interface

4. Enter the login username and password. If this is the first time you are logging in or you have not previously configured the password for the "root" or "admin" accounts, you can use one of the default account details to log in.

ADMIN MANAGER ACCOUNT		ROOT MANAGER ACCOUNT	
Username:	admin	Username:	root
Password:	admin	Password:	admin

Table 9 - Management account login details

Note: To access all features of the router, you must use the root manager account.
For security reasons, we highly recommend that you change the passwords for the root and admin accounts upon initial installation. You can do so by navigating via the menu to the System and then Administration page.

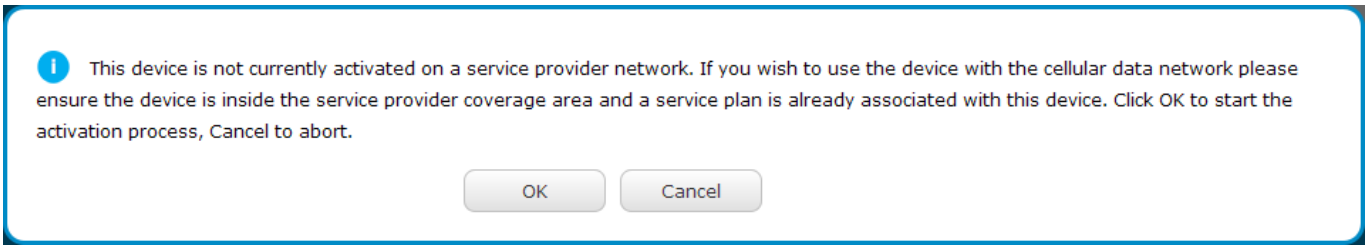
5. The Status page is displayed when you log in successfully.

Activating the router

Before you can use your NWL-15 router, a broadband plan must first be added to it. To add a service to your NWL-15 router, contact your wireless operator (e.g. Verizon Wireless). You will need to provide the wireless operator with the MEID of your router to provision a service. The MEID of your router is printed on the box and the label affixed to the bottom of the router. After the wireless operator has provisioned the service, you may proceed to activate the NWL-15 router on the network.

To perform the activation process:

1. Log in to the router as described above. The Status page is displayed and the router prompts you to activate it by displaying the following pop-up window:
2.


This device is not currently activated on a service provider network. If you wish to use the device with the cellular data network please ensure the device is inside the service provider coverage area and a service plan is already associated with this device. Click OK to start the activation process, Cancel to abort.
OK
Cancel

3. Click the **OK** button on the pop-up window. The router displays "Programming In Progress". Wait approximately 2 minutes for the activation process to complete.

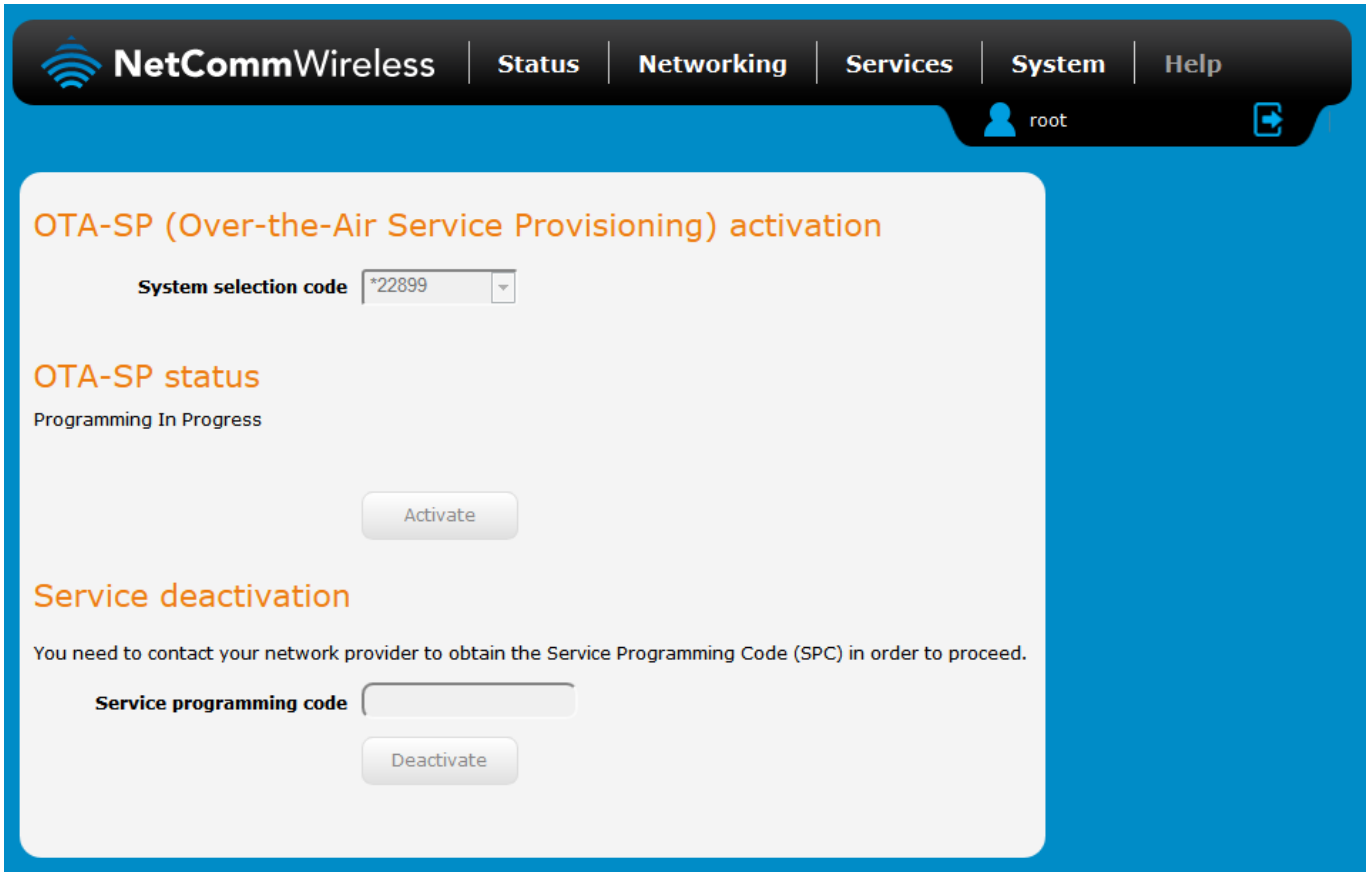


Figure 18: Activation - Programming In Progress

When the activation process is complete, the router displays the Status page. The word **Activated** appears in the **Activation Status** field on the Status page. Your NWL-15 router is now activated and ready for use. For advanced configuration, see the following sections of this guide.

Advanced configuration

The NWL-15 router comes with preconfigured settings that should suit most customers. For advanced configuration, log in to the web-based user interface of the router as described in the previous section. The following sections detail the advanced configuration options available on the NWL-15 router.

Status

The status page of the web interface provides system related information and is displayed when you log in to the NWL-15 router management console. The status page shows System information, LAN details, Cellular connection status, Packet data connection status and Advanced status details. You can toggle the sections from view by clicking the or buttons to show or hide them. Extra status boxes will appear as additional software features are enabled (e.g. VPN connectivity).

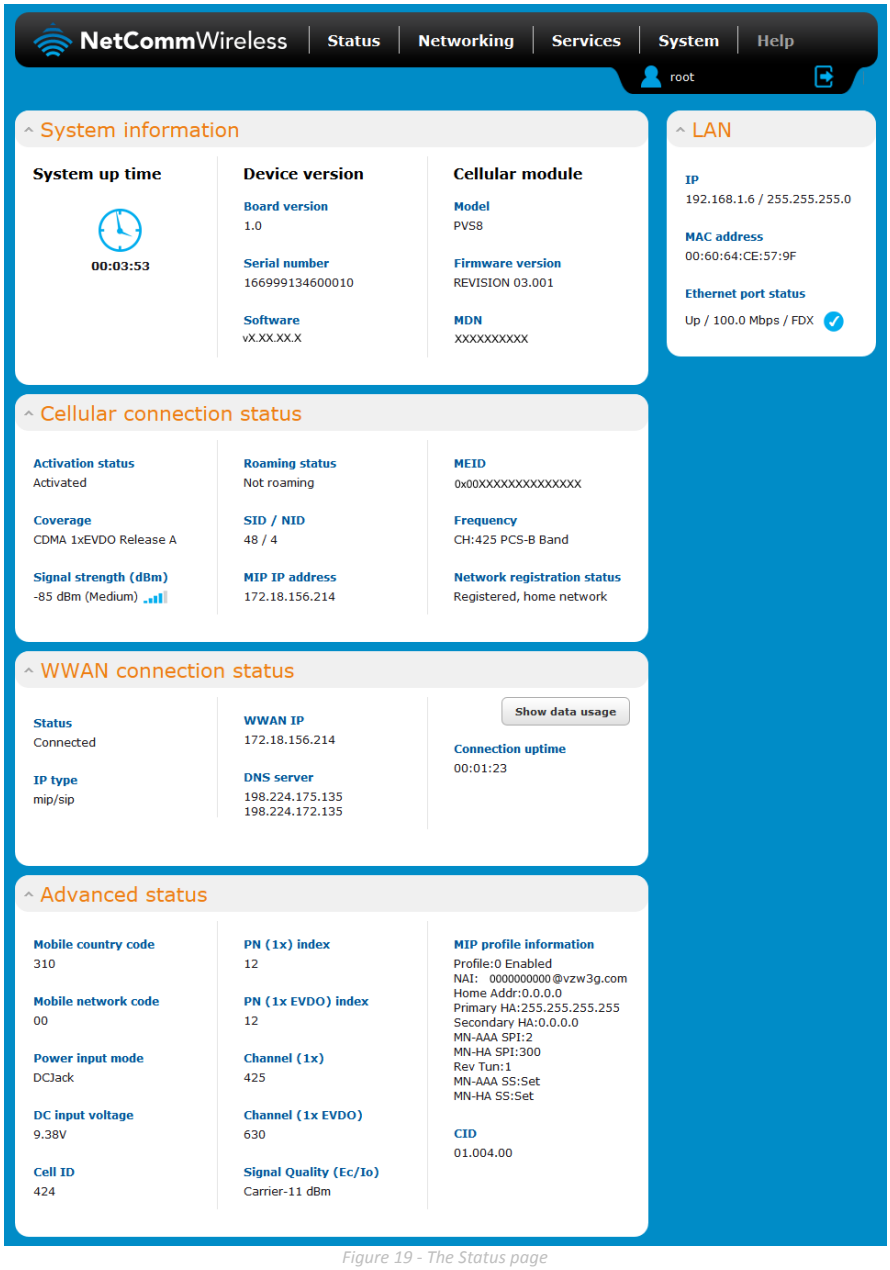


Figure 19 - The Status page

ITEM	DEFINITION
System information	
System up time	The current uptime of the router.
Board version	The hardware version of the router.
Router Serial Number	The serial number of the router.
Software	The software version number running on the router.
Model	The type of phone module and the firmware version of the module.
Firmware	The firmware revision of the phone module.
MDN	The Mobile Directory Number of the router on the network.
LAN	
IP	The IP address and subnet mask of the router.
MAC Address	The MAC address of the router.
Ethernet Port Status	Displays the current status of the Ethernet port and its operating speed.
Cellular connection status	
Activation Status	Displays the activation status of the router on the carrier network.
Coverage	Indicates the type of coverage being received by the router's antennas.
Signal strength (dBm)	The current signal strength measured in dBm
Roaming status	The roaming status of the router.
SID / NID	The System ID and Network ID of the router.
MIP IP Address	The Mobile IP Address.
MEID	The mobile equipment identifier (MEID) of the router, a unique code for identifying devices on a CDMA network.
Frequency	The channel that the router is using on the mobile network.
Network Registration Status	The status of the router's registration for the current network.
WWAN Connection Status	
Status	The connection status of the active profile.
IP Type	The type of IP in use. SIP is a Simple IP connection and when moving between cell sectors, the PPP session is torn down. MIP is a Mobile IP connection which creates an address which is persistent between across cell sectors allowing the mobile connection to remain connected even when moving between cell sectors.
WWAN IP	The IP address assigned by the mobile broadband carrier network.
DNS server	The primary and secondary DNS servers for the WWAN connection.
Connection uptime	The length of time of the current mobile connection session.
Advanced status	
Mobile Country Code	The Mobile Country Code (MCC) of the router.
Mobile Network Code	The Mobile Network Code (MNC) of the router.
Power Input Mode	Displays the router's power source.
DC Input Voltage	Displays the current voltage of the power input source provided via the DC Input jack
Cell ID	A unique code that identifies the base station from within the location area of the current mobile network signal.
PN (1x) Index	The pseudo-random number index used in encrypting the mobile connection for RTT connections.
PN (1x EVDO) Index	The pseudo-random number index used in encrypting the mobile connection for EVDO connections.
Channel (1x)	The 1x (RTT) channel number in use.
Channel (1x EVDO)	The 1x (EVDO) channel number in use.
Signal quality (Ec/Io)	A measurement of the portion of the received signal that is usable. This is the signal strength minus the signal noise level.
MIP Profile Information	Displays various details about the profile used to connect to the broadband network.

Table 10 - Status page item details

Networking

The Networking section provides configuration options for Wireless WAN, LAN, Routing and VPN connectivity.

Data connection

The data connection page allows you to configure and enable/disable the connection profile. To access this page, click on the Internet menu, and under the Wireless WAN menu, select the Data Connection item.

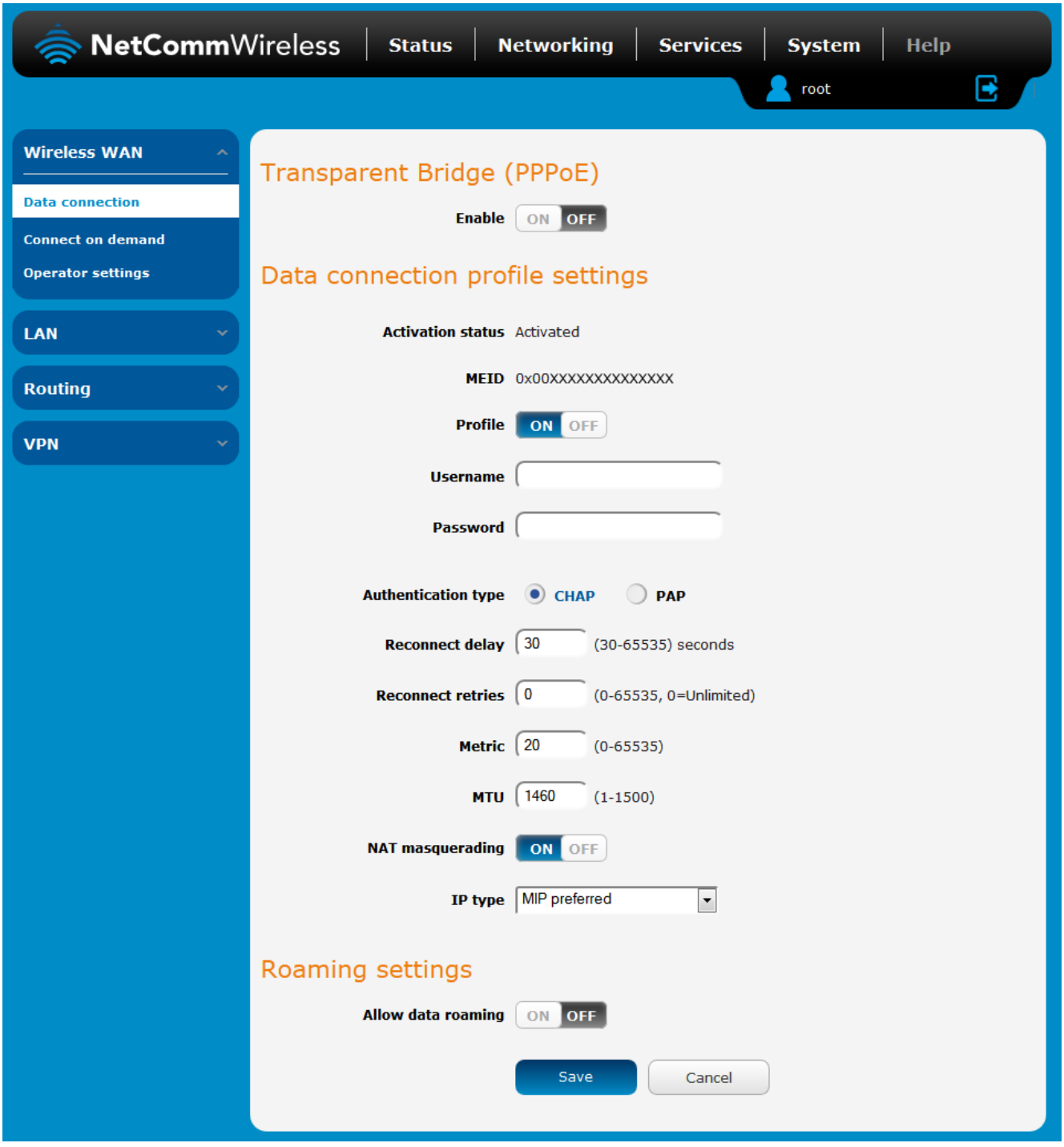


Figure 20 – Data connection settings

ITEM	DEFINITION
Transparent Bridge (PPPoE)	
Enable	Turns on/off the transparent bridge mode of the router.
Data connection profile settings	
Activation Status	Shows whether the router has been activated on the network.
MEID	The mobile equipment identifier (MEID) of the router, a unique code for identifying devices on a CDMA network.
Profile	Toggles the WWAN connection on and off.
User	The CDMA username provided for the router by your carrier.
Password	The CDMA password provided for the router by your carrier.
Authentication Type	The protocol used for authenticating the user on the network.
Reconnect Delay	The time to wait between connection attempts when a connection has been dropped or connection failed.
Reconnect Retries	The number of times to retry to establish a connection when a connection has been dropped or connection failed.
Metric	The metric value is used by the router to prioritise routes. The lower the value, the higher the priority. To give the route the highest priority, set it to 0.
MTU	The maximum transmission uni (MTU) size. The default value is 1460. You should not change this value unless instructed to by your network provider.
NAT Masquerading	NAT masquerading, also known simply as NAT is a common routing feature which allows multiple LAN devices to appear as a single WAN IP via network address translation. In this mode, the router modifies network traffic sent and received to inform remote computers on the internet that packets originating from a machine behind the router actually originated from the WAN IP address of the router's internal NAT IP address.
IP Type	The type of IP in use. SIP is a Simple IP connection and when moving between cell sectors, the PPP session is torn down. MIP is a Mobile IP connection which creates an address which is persistent between across cell sectors allowing the mobile connection to remain connected even when moving between cell sectors.
Roaming settings	
Allow data roaming	Toggles on/off the ability to roam to networks other than the one the router was activated on.

Table 11 - Data connection item details

If your device has not yet been activated on the carrier network, the activation status and MEID are displayed.

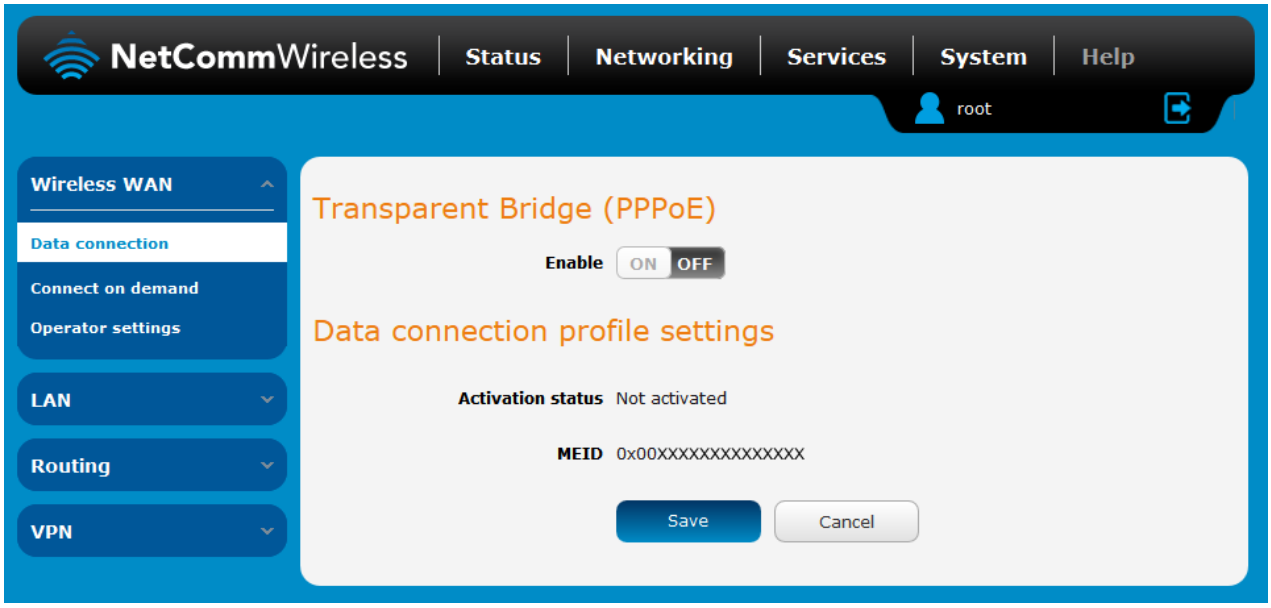


Figure 21 - Device not activated

Refer to the Activating the router section to activate your router on the network.

Manually configuring a connection profile

To manually configure a connection profile:

1. Click the **Profile** toggle key to turn the profile **ON**. Additional settings appear.

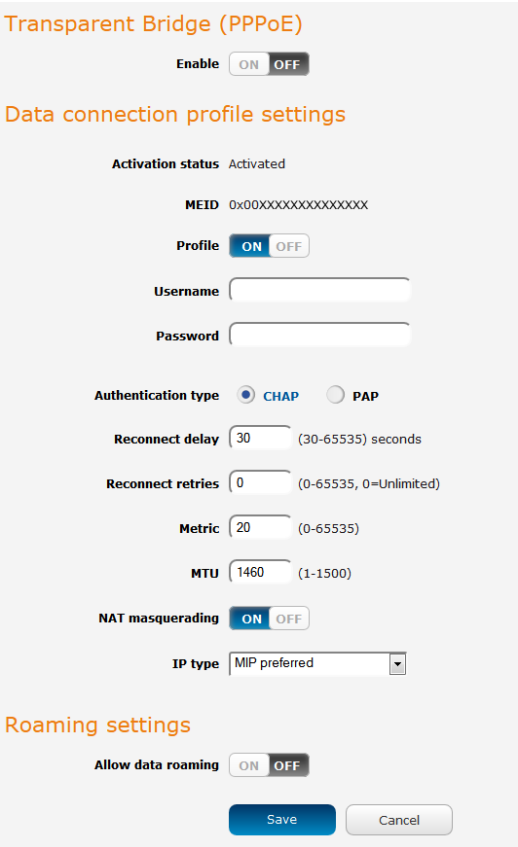


Figure 22 - Data connection settings - Profile turned on

2. In the **User** and **Password** fields, enter the username and passwords assigned to your account by the carrier.
3. Next to **Authentication Type**, select CHAP or PAP depending on the type of authentication used by your provider.
4. The **Reconnect Delay** field specifies the number of seconds to wait between connection attempts. The default setting of 30 seconds is sufficient in most cases but you may modify it to wait up to 65535 seconds if you wish.
5. The **Reconnect Retries** field specifies the number of times to attempt to connect to the network if the router fails to establish a connection. It is set to 0 by default which causes the router to attempt to reconnect indefinitely.
6. The **Metric** value is used by router to prioritise routes (if multiple are available) and is set to 20 by default. This value is sufficient in most cases but you may modify it if you are aware of the effect your changes will have on the service.
7. The **MTU** field specifies the maximum transmission unit which is the largest packet or frame that can be sent in a packet or frame-based network such as the internet. The default value is 1460. This value should only be modified under instruction from your carrier.
8. Use the **NAT Masquerading** toggle key to turn NAT Masquerading on or off. NAT masquerading, also known simply as NAT is a common routing feature which allows multiple LAN devices to appear as a single WAN IP via network address translation. In this mode, the router modifies network traffic sent and received to inform remote computers on the internet that packets originating from a machine behind the router actually originated from the WAN IP address of the router's internal NAT IP address. This may be disabled if a framed route configuration is required and local devices require WAN IP addresses.
9. Use the **IP Type** drop down list to select the type of IP that you want the router to create. **SIP Only** creates a Simple IP via Point-to-Point Protocol and if the router moves between cell sectors, the packet data link is lost. **MIP Only** establishes a Mobile IP connection using an address which is persistent across cell sectors, allowing the router to move between sectors without losing the packet data link. **MIP Preferred** sets the router to use a Mobile IP where possible, but allowing a Simple IP connection if MIP is not available.
10. Click the **Save** button when you have finished entering the profile details.

Confirming a successful connection

After configuring the packet data session, and ensuring that it is enabled, click on the Status menu item at the top of the page to return to the Status page. When there is a mobile broadband connection, the **WWAN** section is expanded showing the details of the connection and the Status field displays **Connected**. To see details on the connected session, you can click the **Show data usage** button.

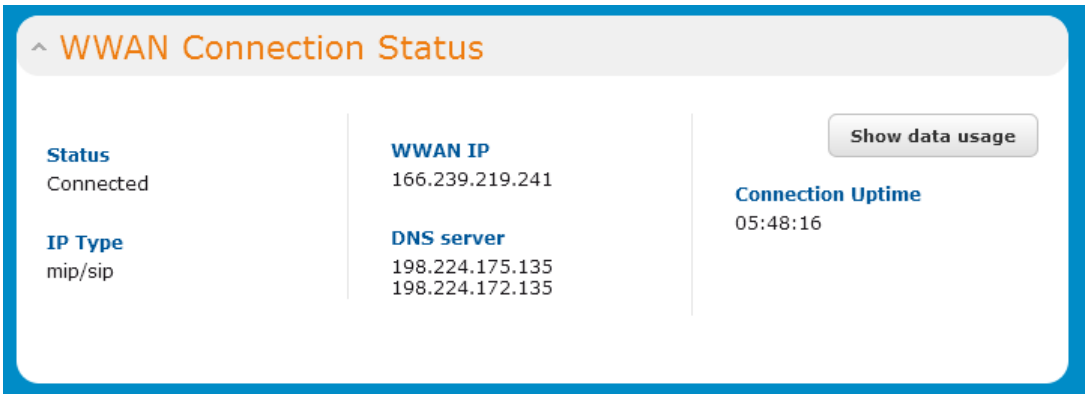


Figure 23 - Packet data connection status section

Transparently bridging the mobile broadband connection via PPPoE

If desired, you can have a client device connected to the Ethernet port initiate the mobile broadband connection using a PPPoE session. This is particularly useful in situations where you wish to provide Wireless WAN data access to an existing router which you want to have full public WAN IP access and have control over routing functionality.

To enable transparent bridging via PPPoE:

1. Click the **Networking** menu item from the top menu bar.
2. On the **Data connection** page, click the **Transparent bridge (PPPoE)** toggle key so that it is **ON**. You are asked to confirm enabling PPPoE, click **OK**. The Transparent Bridge (PPPoE) settings are displayed.

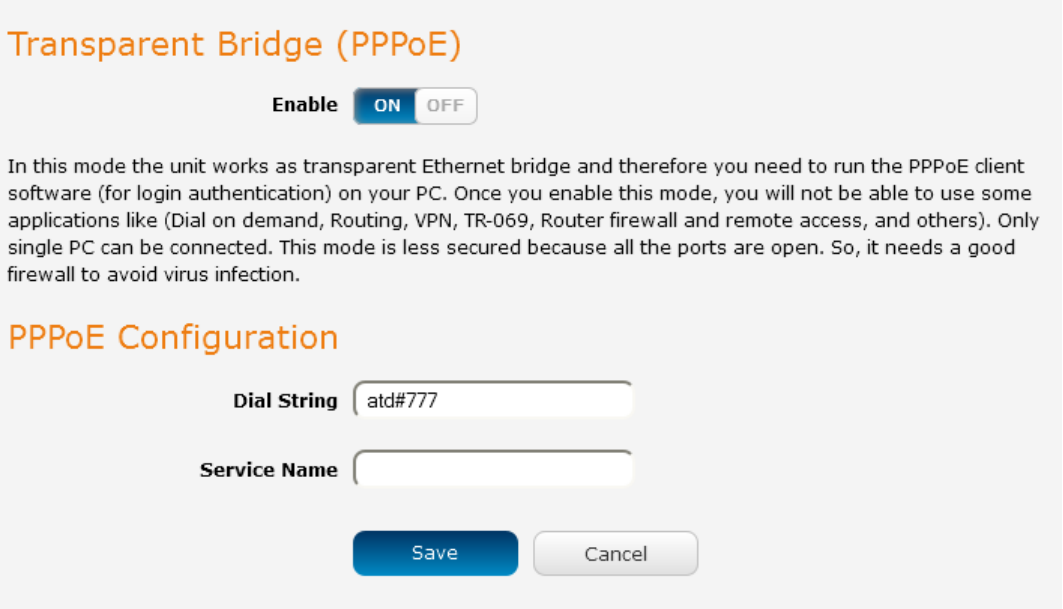

Transparent Bridge (PPPoE)
Enable
ON
OFF
In this mode the unit works as transparent Ethernet bridge and therefore you need to run the PPPoE client software (for login authentication) on your PC. Once you enable this mode, you will not be able to use some applications like (Dial on demand, Routing, VPN, TR-069, Router firewall and remote access, and others). Only single PC can be connected. This mode is less secured because all the ports are open. So, it needs a good firewall to avoid virus infection.
PPPoE Configuration
Dial String
atd#777
Service Name
Save
Cancel

Figure 24 - Transparent bridge configuration

3. In the **Dial String** field, enter the correct dial string for your carrier.
4. (Optional) In the **Service name** field, enter a name that allows you to easily identify the connection.
5. Click the **Save** button to confirm the settings.
6. Click the **Status** menu item from the top menu bar to see the transparent bridging status.

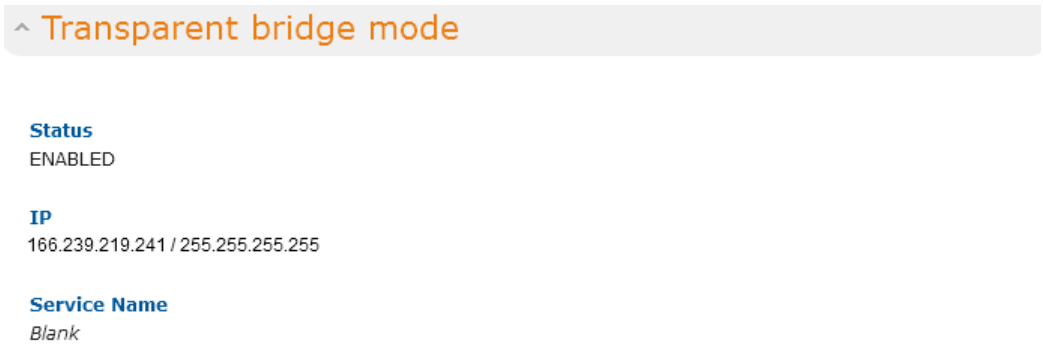


Figure 25 - Transparent bridge mode status

7. Next you must configure your downstream device connected via Ethernet to the NWL-15 router to initiate a network connection through a PPPoE client. The username and password used by the downstream device for the PPPoE session will be passed on and used by the NWL-15 router as the packet data (PDP) context authentication settings.

Connect on demand

The Connect on demand feature keeps the Packet Data Protocol (PDP) context deactivated by default while making it appear to locally connected devices that the router has a permanent connection to the mobile broadband network. When a packet of interest arrives or an SMS wake-up command is received, the router attempts to establish a mobile broadband data connection. When the data connection is established, the router monitors traffic and terminates the link when it is idle.

Note: When interesting packets arrive, the recovery time for the wireless WAN connection is approximately 20-30 seconds.

Configuring Connect on demand

To configure Connect on demand:

1. Click the **Networking** menu item from the top menu bar.
2. On the **Connect on demand** page, click the **Connect on demand** toggle key so that it is **ON**. Extra options appear. See the following sub-sections for further instructions.

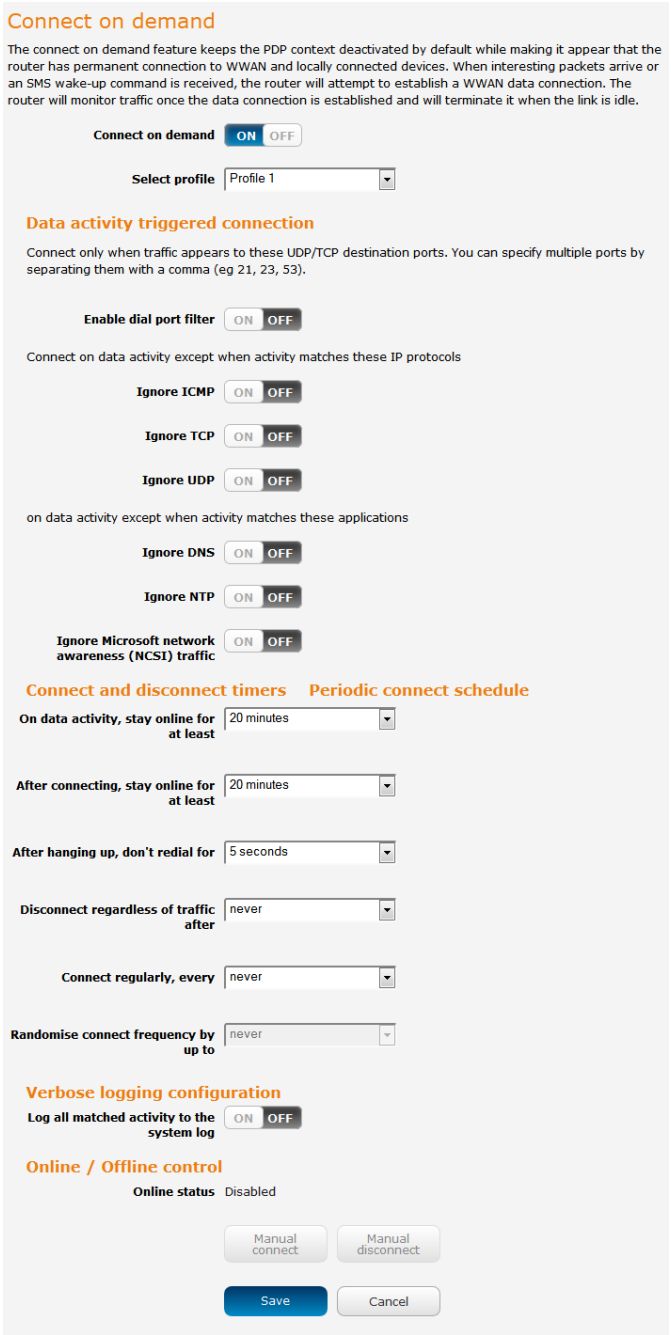

Connect on demand
The connect on demand feature keeps the PDP context deactivated by default while making it appear that the router has permanent connection to WWAN and locally connected devices. When interesting packets arrive or an SMS wake-up command is received, the router will attempt to establish a WWAN data connection. The router will monitor traffic once the data connection is established and will terminate it when the link is idle.
Connect on demand
ON OFF
Select profile
Profile 1
Data activity triggered connection
Connect only when traffic appears to these UDP/TCP destination ports. You can specify multiple ports by separating them with a comma (eg 21, 23, 53).
Enable dial port filter
ON OFF
Connect on data activity except when activity matches these IP protocols
Ignore ICMP
ON OFF
Ignore TCP
ON OFF
Ignore UDP
ON OFF
on data activity except when activity matches these applications
Ignore DNS
ON OFF
Ignore NTP
ON OFF
Ignore Microsoft network awareness (NCSI) traffic
ON OFF
Connect and disconnect timers
Periodic connect schedule
On data activity, stay online for at least
20 minutes
After connecting, stay online for at least
20 minutes
After hanging up, don't redial for
5 seconds
Disconnect regardless of traffic after
never
Connect regularly, every
never
Randomise connect frequency by up to
never
Verbose logging configuration
Log all matched activity to the system log
ON OFF
Online / Offline control
Online status
Disabled
Manual connect
Manual disconnect
Save
Cancel

Figure 26 - Connect on demand configuration options

Setting the router to dial a connection when traffic is detected on specific ports

In some situations, you may wish to have the internet connection disabled except at times when outbound traffic to a particular external host's port or range of ports is sent to the router. To use this feature, click **Enable dial port filter** and enter the port number or list of port numbers separated by commas. When you select this option, all outbound ICMP/TCP/UDP packets to any remote host on the specified port(s) will trigger the connection to dial. Note that when this feature is enabled, the options to ignore specific packet types are not available.

Data activity triggered connection
Connect only when traffic appears to these UDP/TCP destination ports. You can specify multiple ports by separating them with a comma (eg 21, 23, 53).
Enable dial port filter
ON
OFF

Figure 27 – Connect on demand - Data activity triggered connection

You can allow Microsoft network awareness (NCSI) traffic through but if you prefer that they do not trigger the connection, click the **Ignore Microsoft network awareness (NCSI) traffic** toggle key to set it to **ON**.

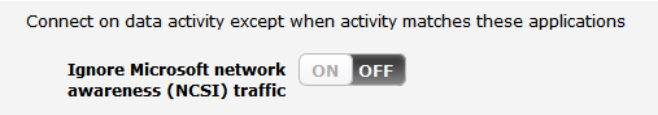

Connect on data activity except when activity matches these applications
Ignore Microsoft network awareness (NCSI) traffic
ON
OFF

Figure 28 - Connect on demand - Ignore NCSI traffic

Excluding certain packet types from triggering the connection to dial

Depending on your environment, you might prefer to exclude certain types of traffic passing through the router from triggering the data connection. You can tell the router to ignore outbound TCP, UDP or ICMP packets. When any of these options are checked the router will not dial a connection when that type of outbound destined data packet reaches the router from a locally connected device.

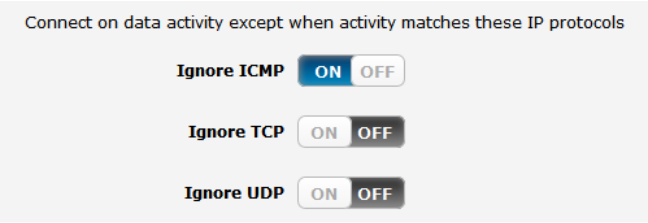


Figure 29 – Connect on demand - Excluding IP protocols

Excluding certain application types from triggering the connection to dial

Some devices may generate general traffic as a part of normal operation which you may not want to trigger the data connection. You can set the router to ignore Domain Name System (DNS), Network Time Protocol (NTP) or Microsoft network awareness (NCSI) traffic from devices behind the router. When you check the box for these options, it tells the router to ignore the request from that application type and will not dial a connection when this data type is received.

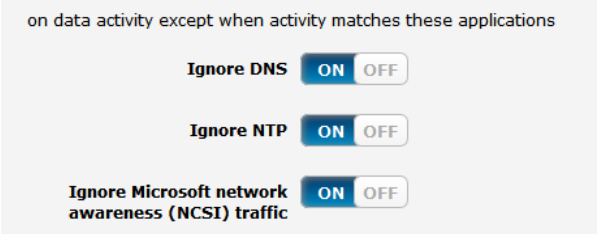


Figure 30 - Connect on demand - Excluding application types

Setting timers for dial-up and disconnection

The router has a number of timer settings which let you determine when a connection is dialled and when it is disconnected.

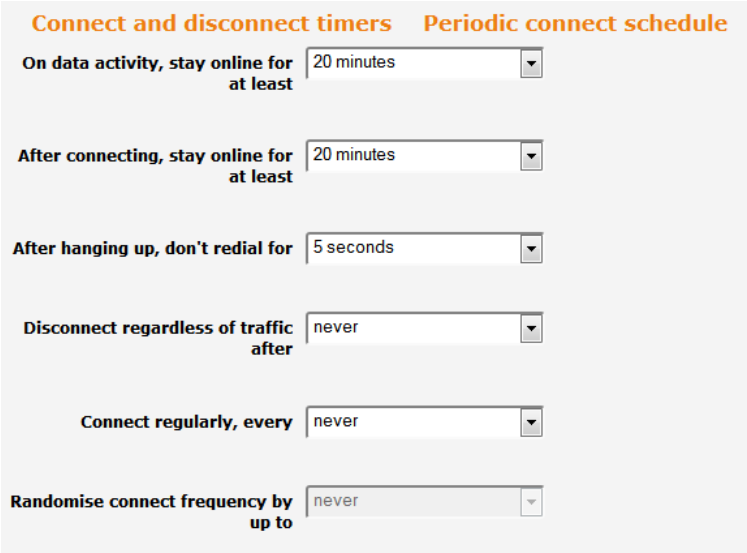


Figure 31 – Connect on demand - Connect and disconnect timers

OPTION	DESCRIPTION
On data activity, stay online for at least	When traffic as per the configured settings above appear, the router will either continue to stay online, or dial a connection and will not disconnect it for the specified time period (min. 1 minute, max. 1 hour). This timer is continuously reset throughout the duration of a dial-up session, whenever data activity is detected matching the rules above.
After connecting, stay online for at least	This timer configures the router to not hang-up the connection for the specified time period after initially dialling the connection. This setting cannot be less than the keep online period above. This timer affects the connection only once per dial up session, at the beginning of the session.
After hanging up, don't redial for	After a connection has been disconnected, you can tell the router to rest for a period of time before re-dialling.
Disconnect regardless of traffic after	Forces the router to disconnect the connection regardless of the traffic passing through it. The default setting is *never*.
Connect regularly, every / Randomize connect frequency	If you want to have the router dial a connection at regular intervals, use **Connect regularly, every** to specify the interval between dials. Setting this to *never* effectively disables this option. The router also features the ability to randomize the time at which the first dial action is performed. This is useful in situations such as where you have numerous routers in an area where a power outage has occurred. Setting a random dial time helps to reduce network congestion when all the routers are powered on so they do not all try to connect simultaneously. When **Connect regularly, every** is set to at least 2 minutes, you are able to configure the router to randomize the time it begins to dial. The randomized dial timer only affects the initial dial after the unit powers on or after the settings are saved. For example, if you configure the router to dial every 2 minutes with a randomized connect frequency of 1 minute, the router waits for the **Connect regularly, every** (2 minutes) and then randomly selects a time less than or equal to the **Randomize connect frequency** (1 minute). After the randomly selected time has elapsed, the router dials the connection. After the first dial, the router dials the connection every 2 minutes, ignoring the **Randomize connect frequency** value.

Table 12 - Connect on demand - Connect and disconnect timers descriptions

Verbose mode

The router provides the option of logging all the data activity which matches the settings for the Connect on demand feature for advanced troubleshooting purposes. To enable the logging of the Connect on demand feature, click the **Enable verbose mode** toggle key to switch it **ON**. See the System log section for more information.

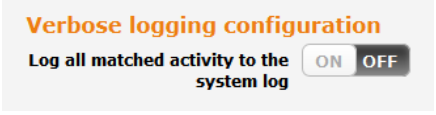


Figure 32 – Connect on demand - Verbose logging configuration

Manually connecting/disconnecting

There may be times when you need to either force a connection to be made or force a disconnection manually. You can use the **Manual connect** and **Manual disconnect** buttons to do this whenever necessary. The online status of the connection is displayed above the buttons.

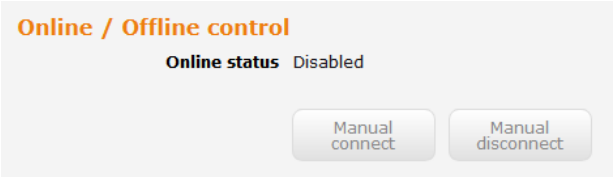


Figure 33 - Connect on demand - Online/Offline control

When you have finished configuring the options for the Connect on demand feature, click the **Save** button at the bottom to save your changes.

Operator settings

The operator settings page lets you configure the roaming preference and mode of the radio.

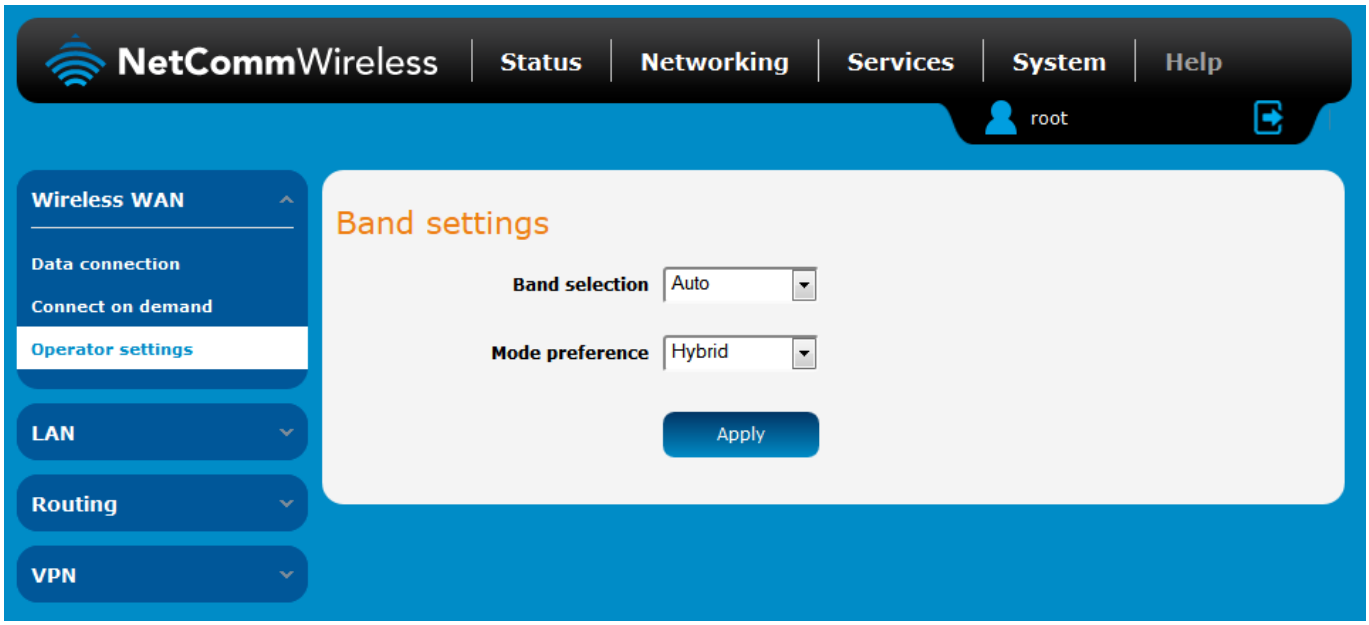


Figure 34 - Band Settings

Band selection

The band selection drop down list provides the ability to select either the A side or B side of the cellular band on which your router is operating. In most cases, the **Auto** setting is sufficient as it automatically selects the best side of the band in your area. You should not change this setting from the default Auto setting unless you are instructed to by your carrier.

Mode preference

The Mode Preference drop down list allows you to select the radio transmission technology used for network access. This affects the quality and speed of network access. The default setting of **Hybrid** is appropriate for most users as it automatically selects the fastest network. If you need to restrict the router to a particular mode, select either **1x Only** or **HDR Only** as per your requirements.

OPTION	DESCRIPTION
1x Only	This is also known as "1xRTT" or 1 times Radio Transmission Technology. It is the version of CDMA2000 radio technology that operates in a pair (transmit and receive) of 1.25 MHz radio channels. It is sometimes referred to as 2.5G
HDR Only	Refers to "1xEVDO" which is also known as Evolution Data Only. This is the third-generation broadband wireless packet data technology optimized for high-speed mobile data.
Hybrid	Automatically selects the best mode for your router based on the signal being received, with preference given to 1xEVDO over 1xRTT. When 1xEVDO is unavailable, the router falls back to 1xRTT mode.

Table 13 - Band selection options

LAN

LAN configuration

The LAN configuration page is used to configure the LAN settings of the router and to enable or disable DNS Masquerading.

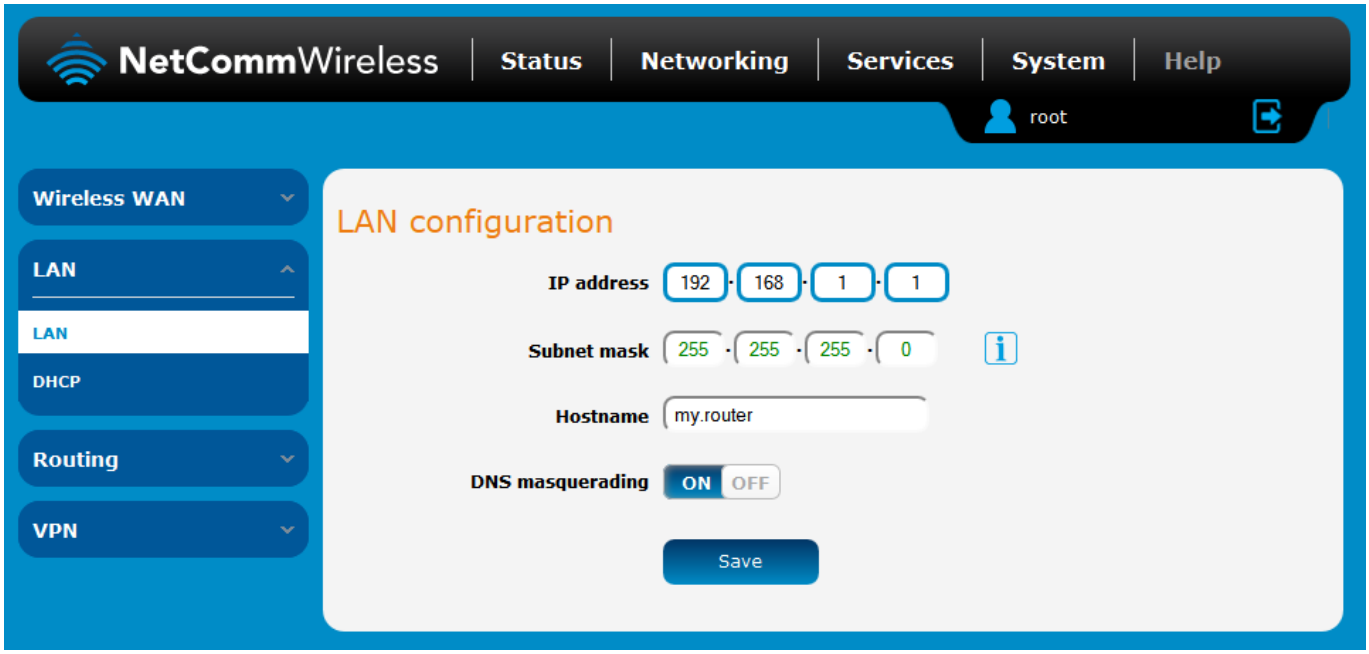


Figure 35 – LAN configuration settings

The default IP of the Ethernet port is 192.168.1.1 with subnet mask 255.255.255.0. To change the IP address or Subnet mask, enter the new IP Address and/or Subnet mask and click the **Save** button.

Note: If you change the IP address, remember to reboot the router and enter the new IP address into your browser address bar.

DNS masquerading

DNS masquerading allows the router to proxy DNS requests from LAN clients to dynamically assigned DNS servers. When enabled, clients on the router's LAN can then use the router as a DNS server without needing to know the dynamically assigned cellular network DNS servers.

With DNS masquerading **ON**, the DHCP server embedded in the NWL-15 router hands out its own IP address (e.g. 192.168.1.1) as the DNS server address to LAN clients. The downstream clients then send DNS requests to the NWL-15 router which proxies them to the upstream DNS servers.

With DNS masquerading **OFF**, the DHCP server hands out the upstream DNS server IP addresses to downstream clients directly, so that downstream clients send DNS requests directly to the upstream DNS servers without being proxied by the NWL-15 router.

You may also override the DNS Masquerading option by specifying custom DNS Server IP addresses in the DHCP Server configuration mentioned in the next section of this guide. In this case the DHCP server assigns downstream devices the manually configured addresses and the DNS Masquerading option is ignored.

In most cases, it is not necessary to disable DNS masquerading but if you need to, click the **DNS masquerading** toggle key to turn it **OFF** and then click the **Save** button.

DHCP

The DHCP page is used to adjust the settings used by the router's built in DHPC Server which assigns IP addresses to locally connected devices.

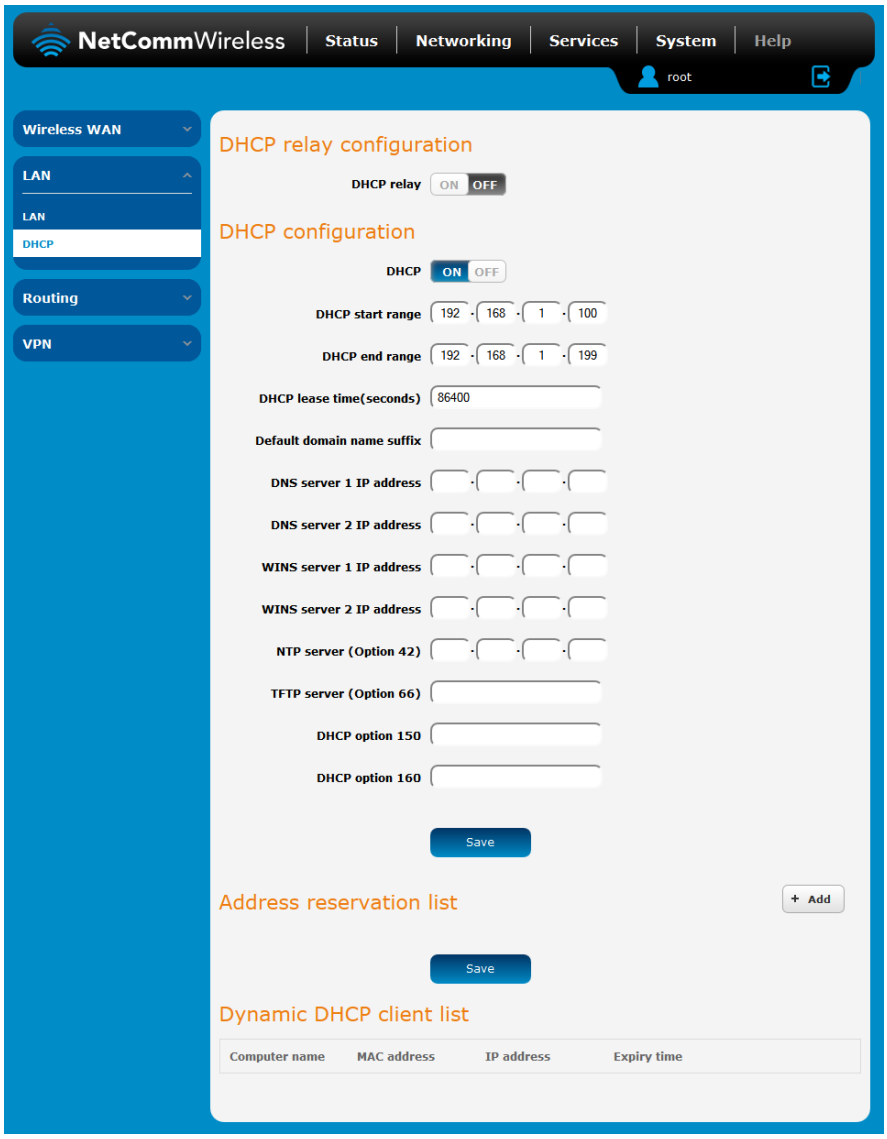


Figure 36 - DHCP Configuration

DHCP relay configuration

In advanced networks configurations where the NWL-15 router should not be responsible for DHCP assignment, but instead an existing DHCP server is located on the Wireless WAN connection, the clients behind the NWL-15 router are able to communicate with the DHCP server when DHCP relay is enabled. This enables the NWL-15 router to accept client broadcast messages and to forward them onto another subnet.

To configure the router to act as a DHCP relay agent click the **DHCP Relay** toggle key to turn it **ON** and enter the DHCP server address into the **DHCP Server Address** field. DHCP relay is disabled by default.

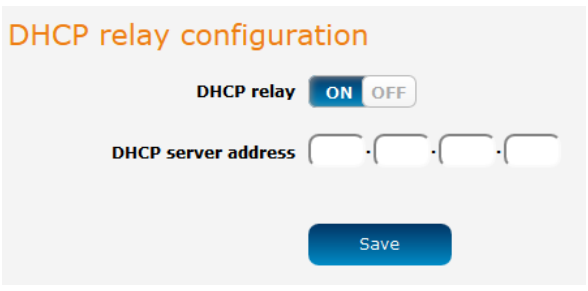


Figure 37 – DHCP relay configuration

DHCP configuration

You can manually set the start and end address range to be used to automatically assign addresses within, the lease time of the assigned address, the default domain name suffix, primary and secondary DNS server, the primary and secondary WINS server, as well as the advanced DHCP settings such as NTP, TFTP and Option 150/Option 160 (VoIP options).

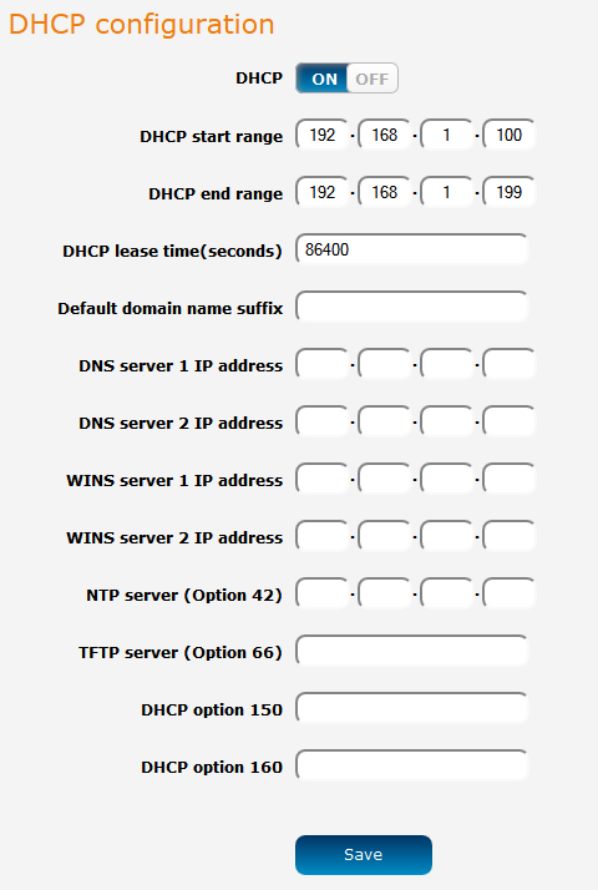


Figure 38 - DHCP configuration

OPTION	DESCRIPTION
DHCP Start Range	Sets the first IP address of the DHCP range
DHCP End Range	Sets the last IP address of the DHCP range
DHCP Lease Time (seconds)	The length of time in seconds that DHCP allocated IP addresses are valid
Default Domain Name Suffix	Specifies the default domain name suffix for the DHCP clients. A domain name suffix enables users to access a local server, for example, server1, without typing the full domain name server1.domain.com
DNS Server 1 IP Address	Specifies the primary DNS (Domain Name System) server's IP address.
DNS Server 2 IP Address	Specifies the secondary DNS (Domain Name System) server's IP address.
WINS Server 1 IP Address	Specifies the primary WINS (Windows Internet Name Service) server IP address
WINS Server 2 IP Address	Specifies the secondary WINS (Windows Internet Name Service) server IP address
NTP Server (Option 42)	Specifies the IP address of the NTP (Network Time Protocol) server
TFTP Server (Option 66)	Specifies the TFTP (Trivial File Transfer Protocol) server
DHCP Option 150	This is used to configure Cisco IP phones. When a Cisco IP phone starts, if it is not pre-configured with the IP address and TFTP address, it sends a request to the DHCP server to obtain this information. Specify the string which will be sent as a reply to the option 150 request.
DHCP Option 160	This is used to configure Polycom IP phones. When a Polycom IP phone starts, if it is not pre-configured with the IP address and TFTP address, it sends a request to the DHCP server to obtain this information. Specify the string which will be sent as a reply to the option 160 request.

Enter the desired DHCP options and click the **Save** button.

Address reservation list

DHCP clients are dynamically assigned an IP address as they connect, but you can reserve an address for a particular device using the address reservation list.

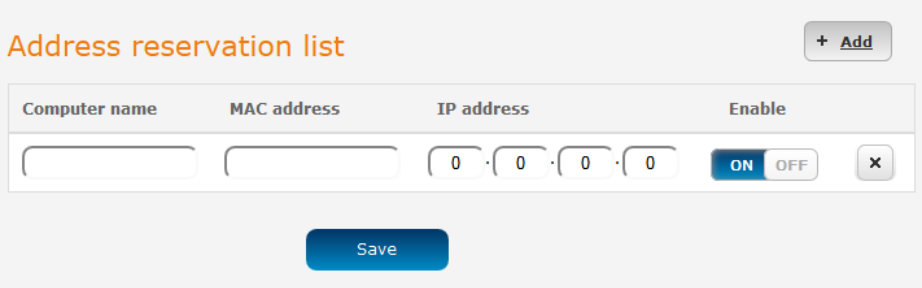


Figure 39 – DHCP – Address reservation list

To add a device to the address reservation list:

1. Click the **+Add** button.
2. In the **Computer Name** field enter a name for the device.
3. In the **MAC Address** field, enter the device's MAC address.
4. In the **IP Address** fields, enter the IP address that you wish to reserve for the device.
5. If the **Enable** toggle key is not set to **ON**, click it to switch it to the **ON** position.
6. Click the **Save** button to save the settings.

Dynamic DHCP client list

The Dynamic DHCP client list displays a list of the DHCP clients. If you want to reserve the current IP address for future use, click the **Clone** button and the details will be copied to the address reservation list fields. Remember to click the **Save** button under the **Address reservation list** section to confirm the configuration.

Figure 40 - Dynamic DHCP client list

Routing

Static

Static routing is the alternative to dynamic routing used in more complex network scenarios and is used to facilitate communication between devices on different networks. Static routing involves configuring the routers in your network with all the information necessary to allow the packets to be forwarded to the correct destination. If you change the IP address of one of the devices in the static route, the route will be broken.

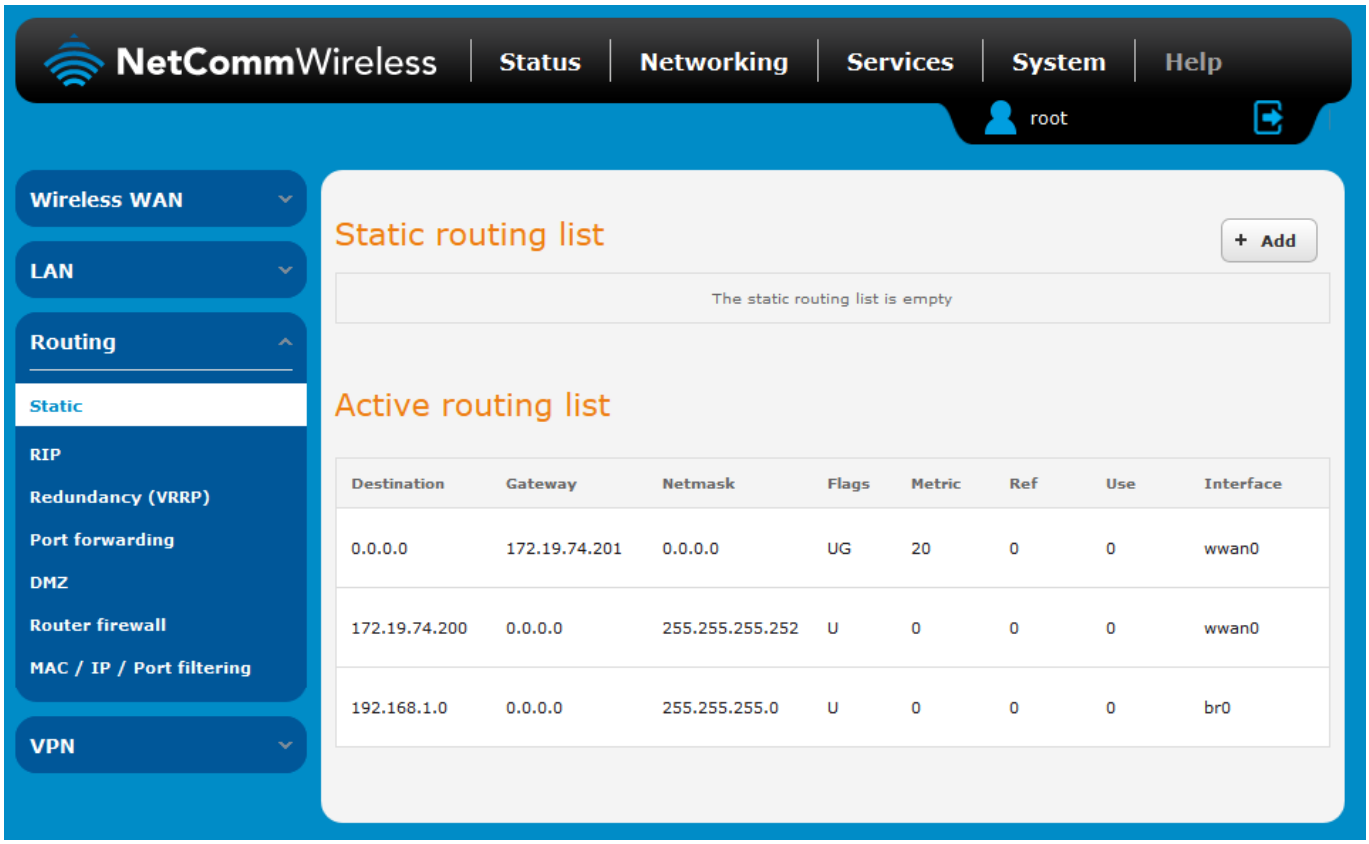


Figure 41 - Static routing list

Some routes are added by default by the router on initialization such as the Ethernet subnet route for routing to a device on the Ethernet subnet.

Adding Static Routes

To add a new route to the static routing list, click the **+Add** button. The Static routes page appears.

1. In the **Route name** field, type a name for the route so that it can be identified in the static routing list.
2. From the **Network interface** drop down list, select the interface for which you would like to create a static route.
3. In the **Destination IP address** field, enter the IP address of the destination of the route.
4. In the **IP subnet mask** field, enter the subnet mask of the route.
5. In the **Gateway IP address** field, enter the IP address of the gateway that will facilitate the route.
6. In the **Metric** field enter the metric for the route. The metric value is used by the router to prioritise routes. The lower the value, the higher the priority. To give the route the highest priority, set it to 0.
7. Click the **Save** button to save your settings.

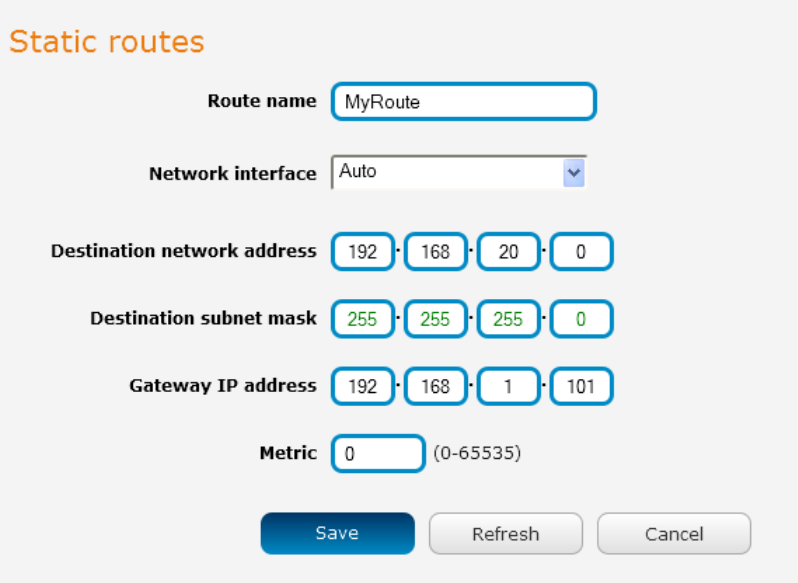
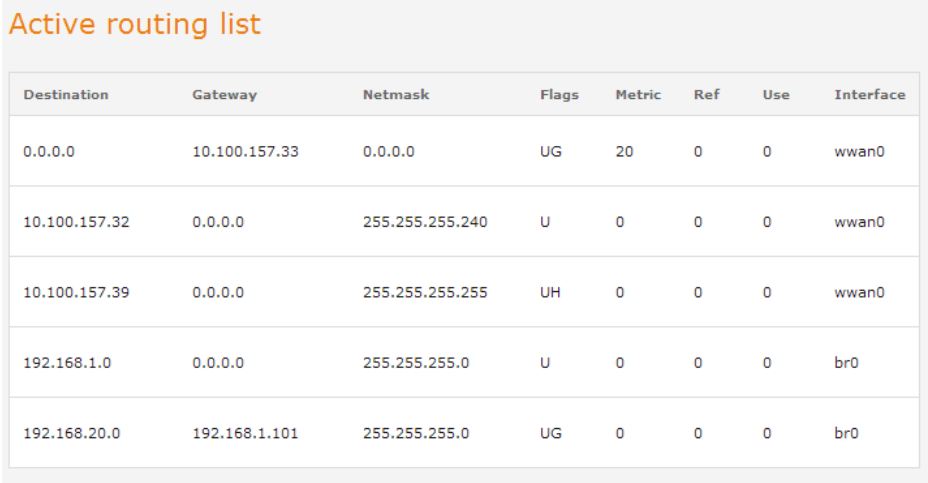


Figure 42 - Adding a static route

Active routing list

Static routes are displayed in the Active routing list.



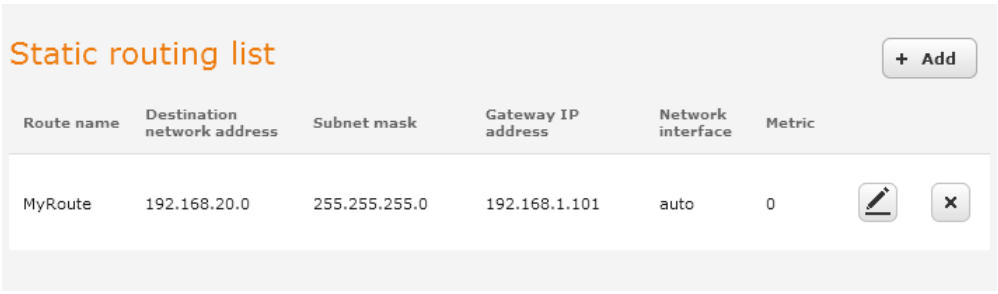
Active routing list

Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
0.0.0.0	10.100.157.33	0.0.0.0	UG	20	0	0	wwan0
10.100.157.32	0.0.0.0	255.255.255.240	U	0	0	0	wwan0
10.100.157.39	0.0.0.0	255.255.255.255	UH	0	0	0	wwan0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
192.168.20.0	192.168.1.101	255.255.255.0	UG	0	0	0	br0

Figure 43 - Active routing list

Deleting static routes

From the static routing list, click the × icon to the right of the entry you wish to delete.



Static routing list

+ Add

Route name	Destination network address	Subnet mask	Gateway IP address	Network interface	Metric		
MyRoute	192.168.20.0	255.255.255.0	192.168.1.101	auto	0		

Figure 44 - Deleting a static route

RIP

RIP (Routing Information Protocol) is used for advertising routes to other routers. Thus all the routes in the router's routing table will be advertised to other nearby routers. For example, the route for the router's Ethernet subnet could be advertised to a router on the PPP interface side so that a router on this network will know how to route to a device on the router's Ethernet subnet. Static routes must be added manually according to your requirements. See Adding Static Routes.

Note: Some routers will ignore RIP.

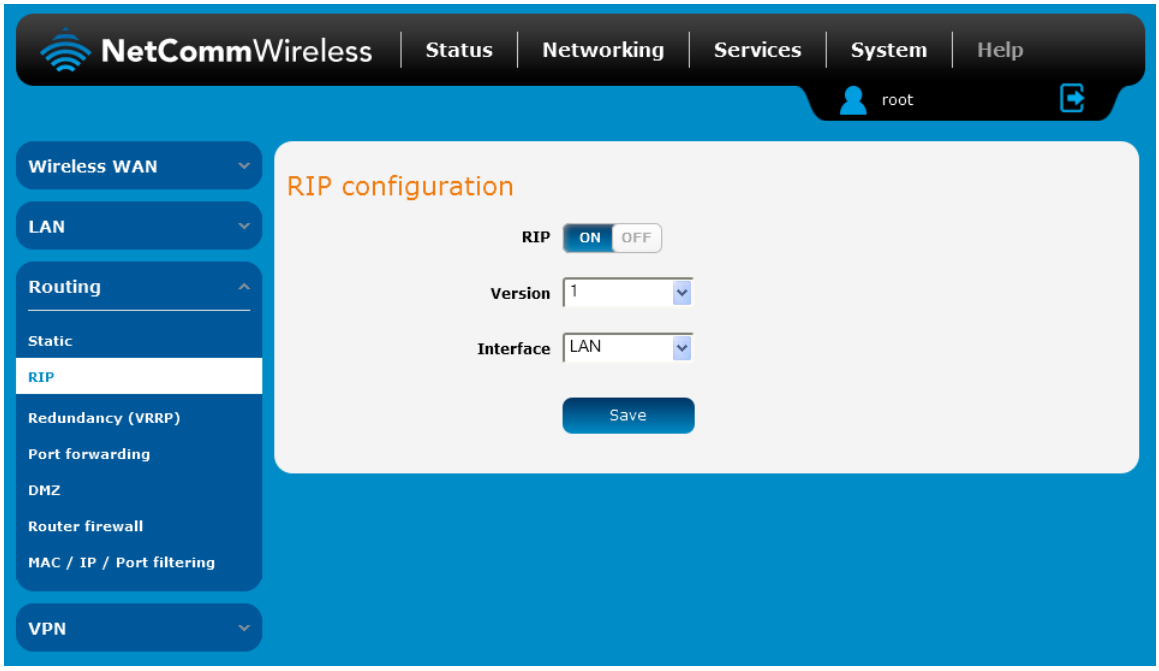


Figure 45 - RIP configuration

To enable Routing Information Protocol (RIP)

1. Click the **RIP** toggle key to switch it to the **ON** position.
2. Using the **Version** drop down list, select the version of RIP that you would like to use.
3. Click the **Save** button to confirm your settings.

VRRP

Virtual Router Redundancy Protocol (VRRP) is a non-proprietary redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. This increased reliability is achieved by advertising a "virtual router" (an abstract representation of master and backup routers acting as a group) as a default gateway to the host(s) instead of one physical router. Two or more physical routers are then configured to stand for the virtual router, with only one doing the actual routing at any given time. If the current physical router that is routing the data on behalf of the virtual router fails, an arrangement is made for another physical router to automatically replace it. The physical router that is currently forwarding data on behalf of the virtual router is called the master router.

Master routers have a priority of 255 and backup router(s) can have a priority between 1 and 254.

A virtual router must use 00-00-5E-00-01-XX as its (MAC) address. The last byte of the address (XX) is the Virtual Router Identifier (VRID), which is different for each virtual router in the network. This address is used by only one physical router at a time, and is the only way that other physical routers can identify the master router within a virtual router.

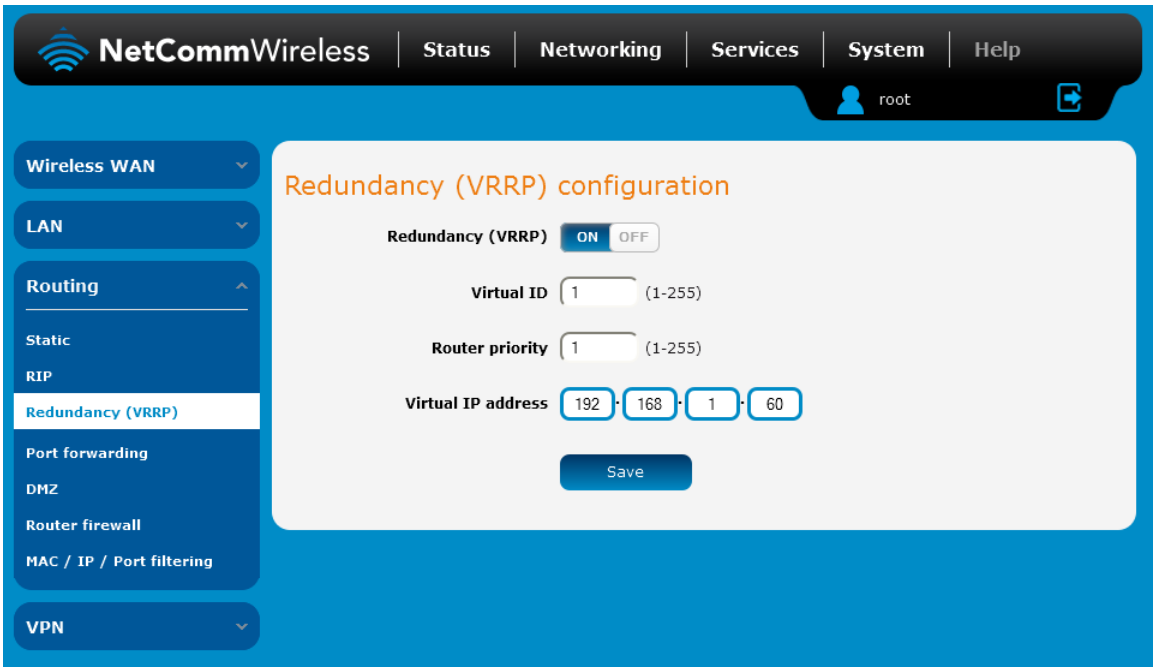


Figure 46 - VRRP configuration

To configure VRRP, configure multiple devices as follows and connect them all via an Ethernet network switch to downstream devices.

1. Click the **Redundancy (VRRP)** toggle key to activate VRRP.
2. In the **Virtual ID** field, enter an ID between 1 and 255. This is the VRRP ID which is different for each virtual router on the network.
3. In the **Router Priority** field, enter a value for the priority – a higher value is a higher priority.
4. The **Virtual IP Address** field is used to specify the VRRP IP address – this is the virtual IP address that both virtual routers share.
5. Click the **Save** button to save the new settings.

Note: Configuring VRRP changes the MAC address of the Ethernet port and therefore if you want to resume with the web configuration you must use the new IP address (VRRP IP) or on a command prompt type:
`arp -d <ip address>` (i.e. `arp -d 192.168.1.1`) to clear the arp cache.(old MAC address).

Port Forwarding

The Port forwarding list is used to configure the Network Address Translation (NAT) rules currently in effect on the router.

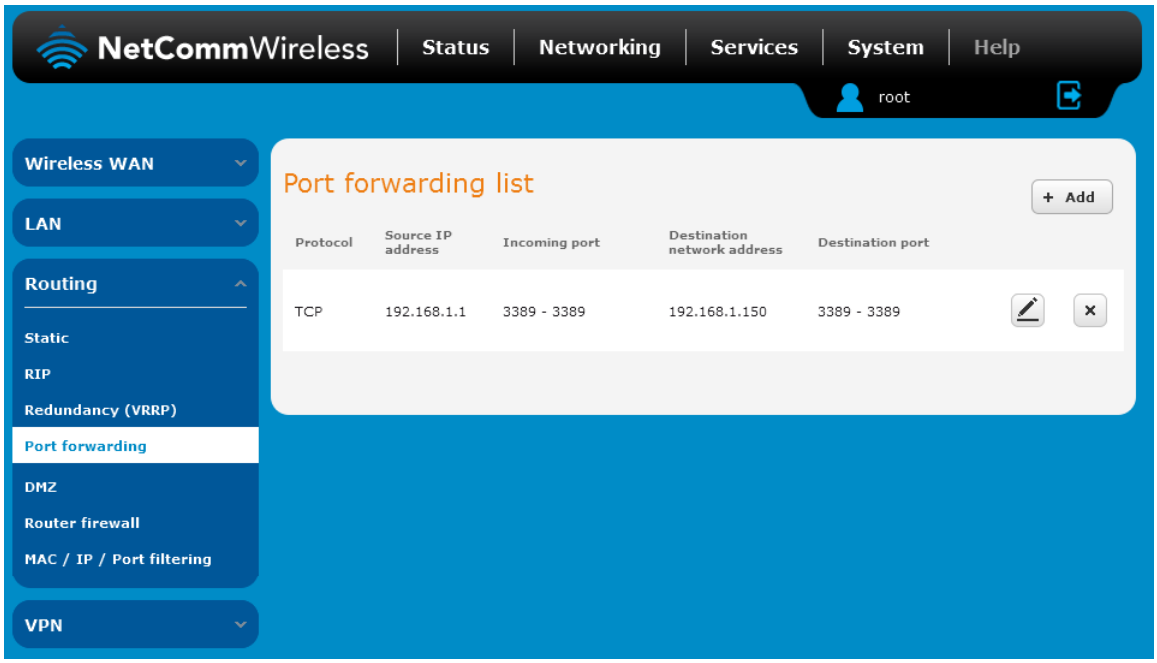


Figure 47 – Port forwarding list

The purpose of the port forwarding feature is to allow mapping of inbound requests to a specific port on the WAN IP address to a device connected on the Ethernet interface.

Adding a port forwarding rule

To create a new port forwarding rule:

1. Click the **+Add** button. The port forwarding settings screen is displayed.
2. Use the **Protocol** drop down list to select the type of protocol you want to use for the rule. The protocols selections available are **TCP, UDP** and **All.**
3. In the **Source IP Address** field, enter a "friendly" address that is allowed to access the router or a wildcard IP address (0.0.0.0) that allows all IP addresses to access the router.
4. The **Source Port Range (From)** and **(To)** fields are used to specify the port(s) on the source side that are to be forwarded. This allows you to send a range of consecutive port numbers by entering the first in the range in the **(From)** field and the last in the range in the **(To)** field. To forward a single port, enter the port in the **(From)** field and repeat it in the **(To)** field.
5. In the **Destination network address** field, enter the IP address of the client to which the traffic should be forwarded.
6. The **Destination Port Range (From)** and **(To)** fields are used to specify the port(s) on the destination side that are to be forwarded. If the Source port range specifies a single port then the destination port may be configured to any port. If the Source port range specifies a range of port numbers then the Destination port range must be the same as the Source port range.
7. Click the **Save** button to confirm your settings.

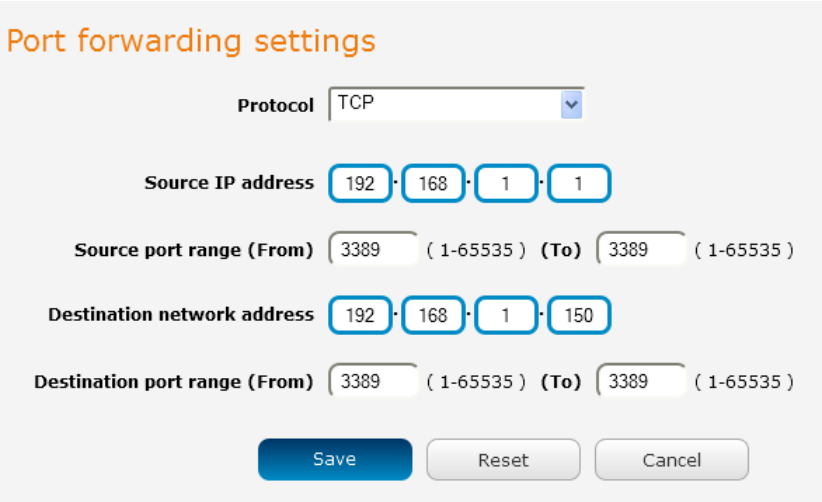


Figure 48 - Port forwarding settings

To delete a port forwarding rule, click the × button on the Port forwarding list for the corresponding rule that you would like to delete.

DMZ

The Demilitarized Zone (DMZ) allows you to configure all incoming traffic on all protocols to be forwarded to a selected device behind the router. This feature can be used to avoid complex port forwarding rules, but it exposes the device to untrusted networks as there is no filtering of what traffic is allowed and what is denied.

The DMZ configuration page is used to specify the IP Address of the device to use as the DMZ host.

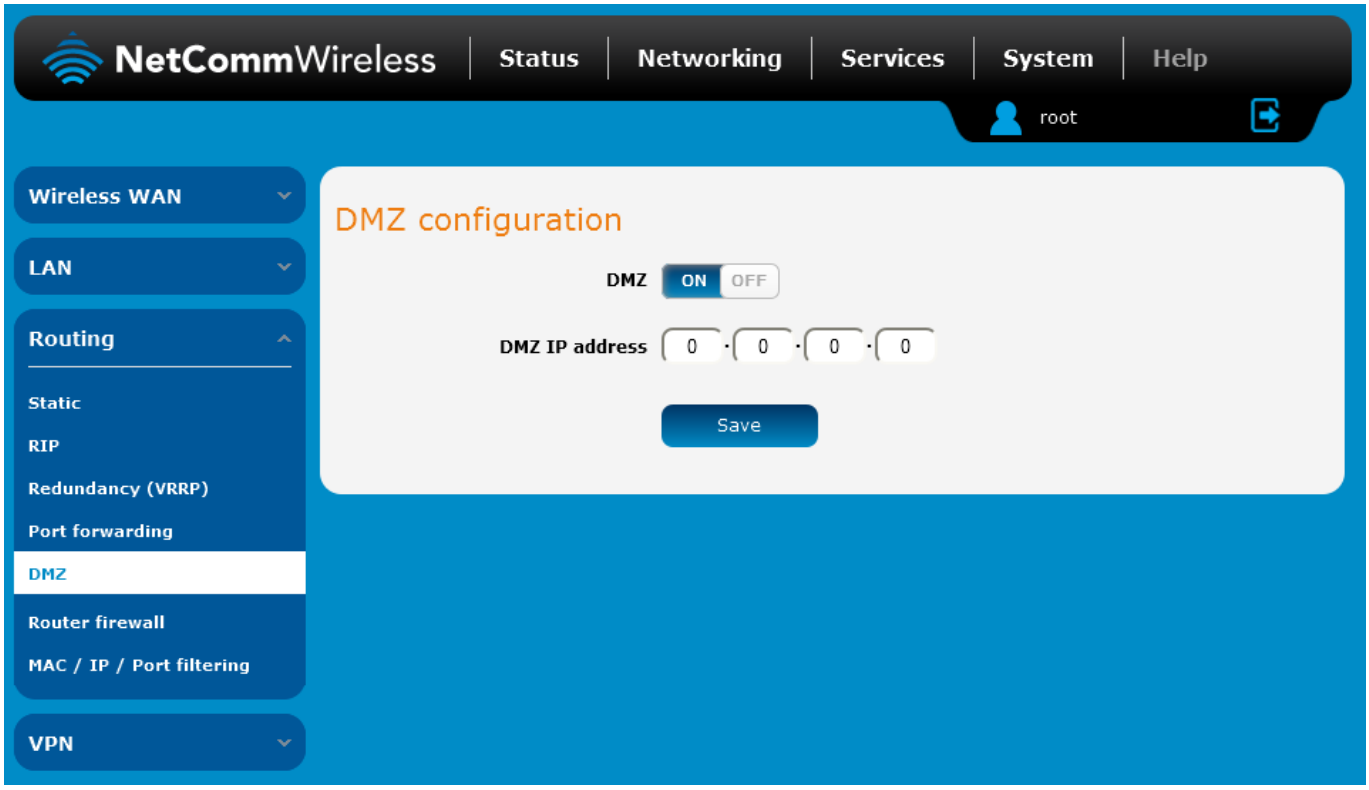


Figure 49 - DMZ configuration

1. Click the DMZ toggle key to turn the DMZ function **ON.**
2. Enter the IP Address of the device to be the DMZ host into the **DMZ IP Address** field.
3. Click the **Save** button to save your settings.

Router firewall

The Router firewall page is used to enable or disable the in-built firewall on the router. When enabled, the firewall performs stateful packet inspection on inbound traffic from the wireless WAN and blocks all unknown services, that is, all services not listed on the Services configuration page of the router.

With respect to the other Routing options on the Internet page, the firewall takes a low priority. The priority of the firewall can be described as:

DMZ > MAC/IP/Port filtering rules > MAC/IP/Port filtering default rule > Router firewall rules

In other words, the firewall is of the lowest priority when compared to other manual routing configurations. Therefore, a MAC/IP/Port filtering rule takes priority in the event that there is a conflict of rules. When DMZ is enabled, MAC/IP/Port filtering rules and the router firewall are ignored but the router will still honor the configuration of the Remote router access control settings listed under Administration Settings.

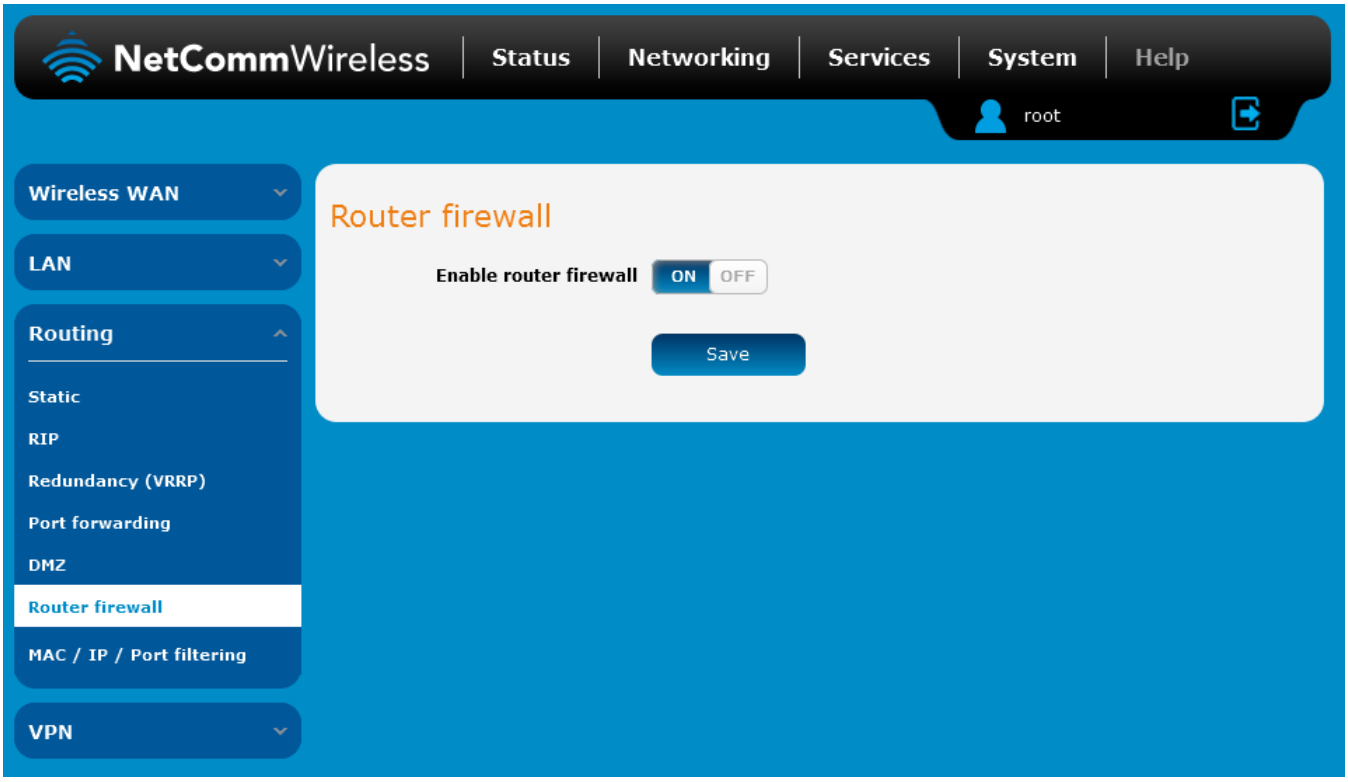


Figure 50 - Router Firewall toggle key

MAC / IP / Port filtering

The MAC/IP/Port filter feature allows you apply a policy to the traffic that passes through the router, both inbound and outbound, so that network access can be controlled. When the filter is enabled with a default rule of "Accepted", all connections will be allowed except those listed in the "Current MAC / IP / Port filtering rules in system" list. Conversely, when the default rule is set to "Dropped", all connections are denied except for those listed in the filtering rules list.

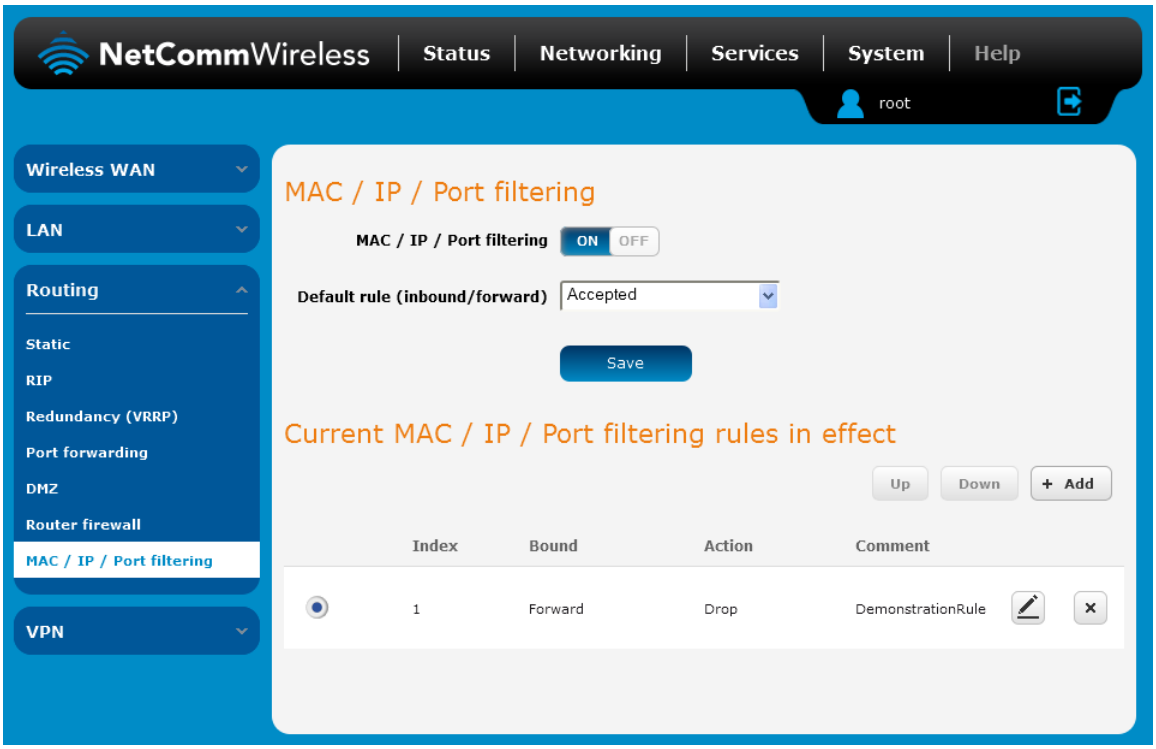


Figure 51 - MAC / IP / Port filtering

Note: When enabling MAC / IP / Port filtering and setting the default rule to "Dropped", you should ensure that you have first added a filtering rule which allows at least one known MAC/IP to access the router, otherwise you will not be able to access the user interface of the router without resetting the router to factory default settings.

Creating a MAC / IP / Port filtering rule

To create a filtering rule:

1. Click the **MAC / IP / Port filtering** toggle key to switch it to the **ON** position.
2. Using the **Default Rule (inbound/forward)** drop down list, select the default action for the router to take when traffic reaches it. By default, this is configured to **Accepted**. If you change this to **Dropped**, you should first configure a filter rule that allows at least one device access to the router, otherwise you will effectively be locked out of the router.
3. Click the **Save** button to confirm the default rule.
4. In the Current MAC / IP / Port filtering rules in system section, click the **+Add** button.

Figure 52 - Current MAC / IP/ Port filtering rules in effect

5. Enter the details of the rule in the section that is displayed and click the **Save** button.

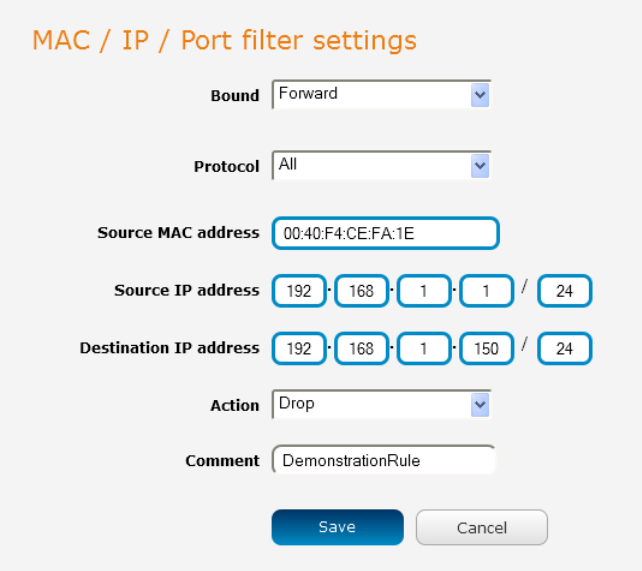


Figure 53 - MAC / IP / Port filtering settings

OPTION	DESCRIPTION
Bound	Use the drop down list to select the direction of the traffic for which you want to apply to the rule. **Inbound** refers to all traffic that is entering the router including data entering from the WAN and the LAN. **Outbound** refers to all traffic exiting the router including traffic leaving in the direction of the WAN and traffic leaving in the direction of the LAN. **Forward** specifies traffic that enters on the LAN or WAN side and is forwarded to the opposite end.
Protocol	Use the drop down list to select the protocol for the rule. You can have the rule apply to **All** protocols, **TCP**, **UDP**, **UDP/TCP** or **ICMP.**
MAC Address	Enter the MAC address in six groups of two hexadecimal digits separated by colons (:). e.g. 00:40:F4:CE:FA:1E
Source IP Address	Enter the IPv4 address that the traffic originates from and the subnet mask using CIDR notation.
Source Port Range (From) – (To)	Only appears for TCP, UDP and UDP/TCP options. Use these fields to specify a port or range of ports from the source side to use for the rule. To specify a single port, repeat it in both the **(From)** and **(To)** fields.
Destination IP Address	Enter the IPv4 address that the traffic is destined for and the subnet mask using CIDR notation.
Destination Port Range (From) – (To)	Only appears for TCP, UDP and UDP/TCP options. Use these fields to specify a port or range of ports on the destination side to use for the rule. To specify a single port, repeat it in both the **(From)** and **(To)** fields.
Action	Select the action to take for traffic which meets the above criteria. You can choose to **Accept** or **Drop** packets. When the default rule is set to **Accept**, you cannot create a rule with an **Accept** action since the rule is redundant. Likewise, if the default rule is set to **Dropped** you cannot create a rule with a **Drop** action.
Comment	[Optional] Use this field to enter a comment as a meaningful description of the rule.

Table 14 - Current MAC / IP / Port filtering rules in effect

6. The new rule is displayed in the filtering rules list. You can edit the rule by clicking the **Edit** button or delete the rule by clicking the × button.

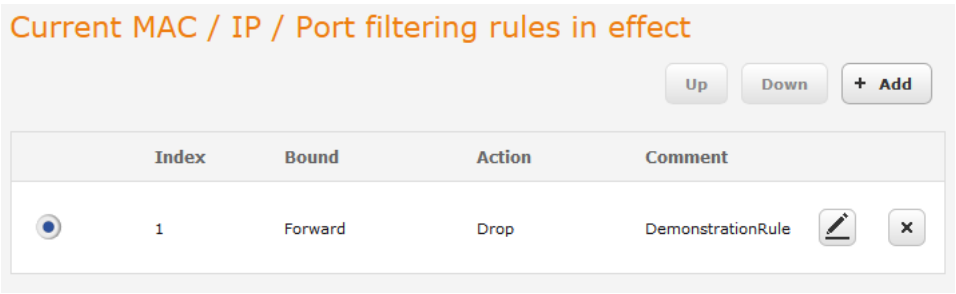


Figure 54 - Completed filtering rule

VPN

A Virtual Private Network (VPN) is a tunnel providing a private link between two networks or devices over a public network. Data to be sent via a VPN needs to be encapsulated and as such is generally not visible to the public network.

The advantages of a VPN connection include:

- Data Protection
- Access Control
- Data Origin Authentication
- Data Integrity

Each VPN connection has different configuration requirements. The following pages detail the configuration options available for the different VPN connection types.

Note: The following descriptions are an overview of the various VPN options available. More detailed instructions are available in separate whitepapers on the NetComm Wireless website.

IPSec

IPSec operates on Layer 3 of the OSI model and as such can protect higher layered protocols. IPSec is used for both site to site VPN and Remote Access VPN. The NWL-15 router supports IPsec end points and can be configured with Site to Site VPN tunnels with third party VPN routers.

Configuring an IPSec VPN

From the menu at the top of the screen, click **Networking** and under the VPN section, click **IPSec**. A list of configured IPSec VPN connections is displayed.

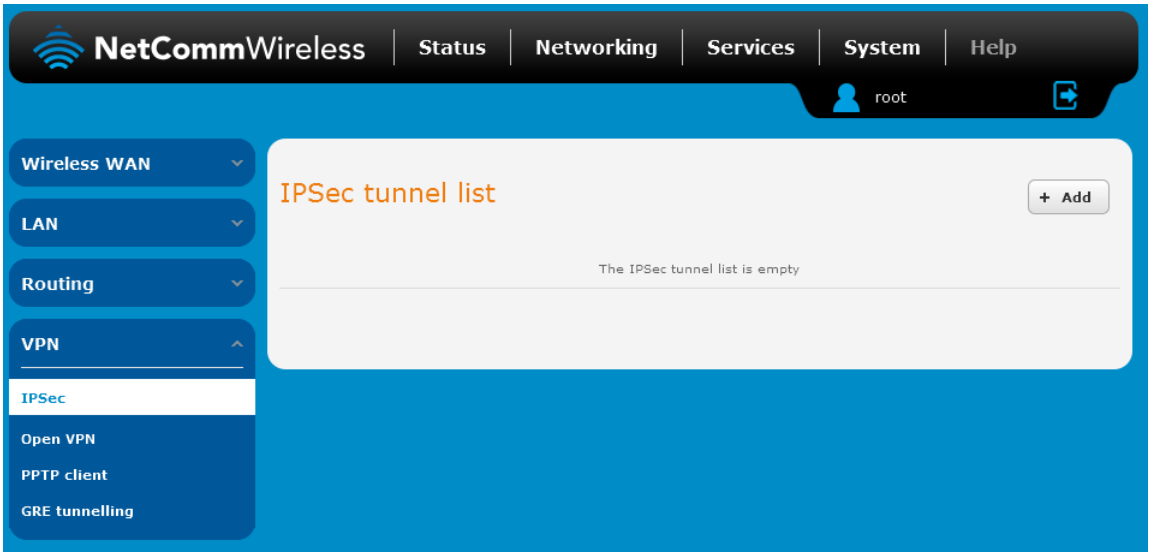


Figure 55 - IPSec VPN List

Click the **+Add** button to begin configuring an IPSec VPN connection.

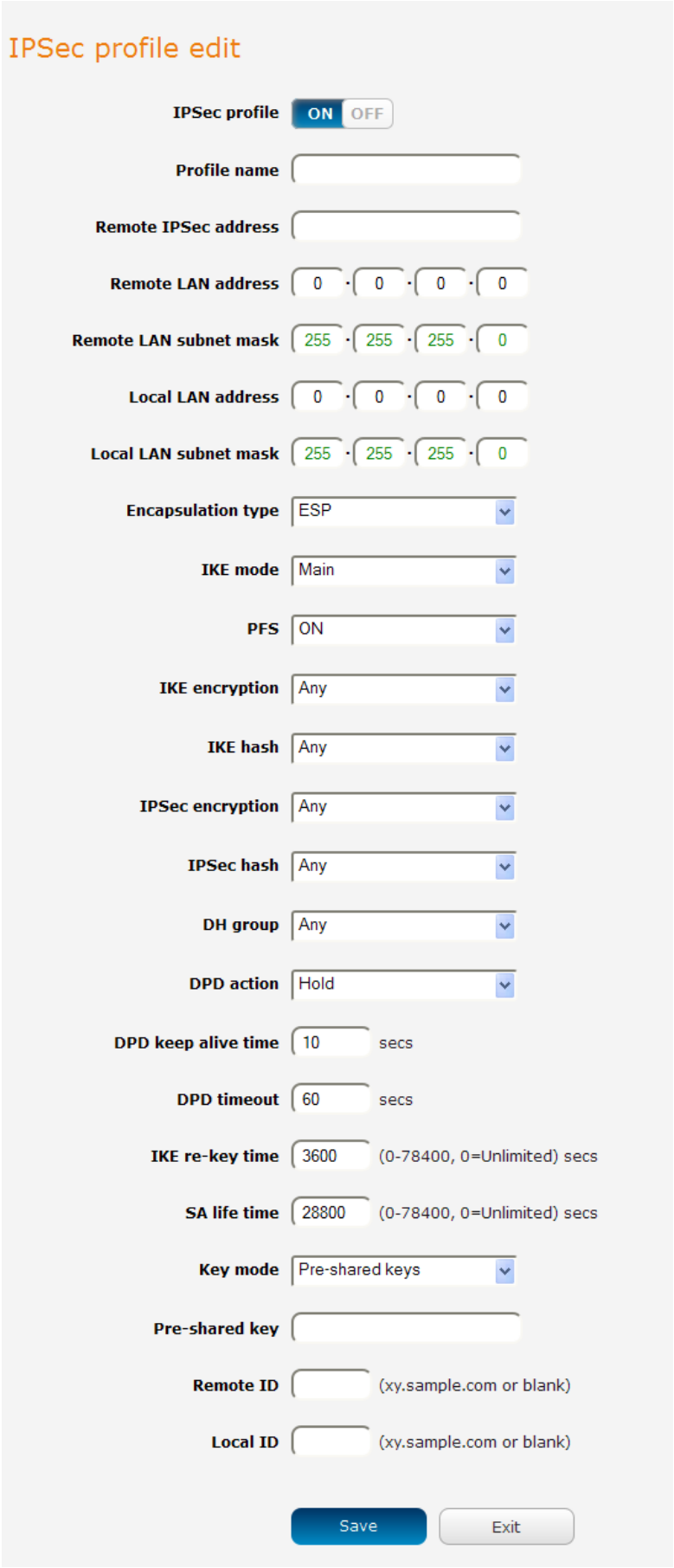


Figure 56 – IPSec profile edit

The following table describes each of the fields of the IPSec VPN Connection Settings page.

ITEM	DEFINITION
IPSec Profile	Enables or disables the VPN profile.
Profile Name	A name used to identify the VPN connection profile.
Remote IPSec Server Address	The IP address of the IPSec server.
Remote LAN Address	Enter the IP address of the remote network for use on the VPN connection.
Remote LAN Subnet Mask	Enter the subnet mask in use on the remote network.
Local LAN Address	Enter the IP address of the local network for use on the VPN connection.
Local LAN Subnet Mask	Enter the subnet mask in use on the local network.
Encapsulation Type	Select the encapsulation protocol to use with the VPN connection. You can choose **ESP**, **AH** or **Any**.
IKE Mode	Select the IKE mode to use with the VPN connection. You can choose **Main**, **Aggressive** or **Any**.
PFS	Choose whether Perfect Forward Secrecy is ON or OFF for the VPN connection.
IKE Encryption	Select the cipher type to use for the Internet Key Exchange.
IKE Hash	Select the IKE Hash type to use for the VPN connection. The hash is used for authentication of packets for the key exchange.
IPSec Encryption	Select the IPSec encryption type to use with the VPN connection.
IPSec Hash	Select the IPSec hash type to use for the VPN connection. The hash is used for authentication of packets for the VPN connection.
DH Group	Select the desired Diffie-Hellman group to use. Higher groups are more secure but also require longer to generate a key.
DPD Action	Select the desired Dead Peer Detection action. This is the action to take when a dead Internet Key Exchange Peer is detected.
DPD Keep Alive Time	Enter the time in seconds for the interval between Dead Peer Detection keep alive messages.
DPD Timeout	Enter the time in seconds of no response from a peer before Dead Peer Detection times out.
IKE Rekey Time	Enter the time in seconds between changes of the encryption key. To disable changing the key, set this to 0.
SA Life Time	Enter the time in seconds for the security association lifetime.
Key Mode	Select the type of key mode in use for the VPN connection. You can select from: 1. Pre Shared Key 2. RSA keys 3. Certificates
Pre-shared Key	The pre-shared key is the key that peers used to authenticate each other for Internet Key Exchange.
Remote ID	Specifies the domain name of the remote network.
Local ID	Specifies the domain name of the local network.
Update Time	Displays the last time the key was updated.
Local RSA Key Upload	Select the RSA key file for the local router here by clicking the **Browse** button.
Remote RSA Key Upload	Select the RSA key file for the remote router here by clicking the **Browse** button.
Private key Passphrase	The Private key passphrase of the router is the passphrase used when generating the router's private key using OpenSSL CA.
Key / Certificate	Select the type of key or certificate to use for authentication. You can select **Local private key**, **Local public certificate**, **Remote public certificate**, **CA certificate**, **CRL certificate**.
IPSec Certificate Upload	Select the IPSec certificate to upload by clicking the **Browse** button.

Table 15 - IPSec Configuration Items

OpenVPN

OpenVPN is an open source virtual private network (VPN) program for creating point-to-point or server-to-multi-client encrypted tunnels between host computers. It can traverse network address translation (NAT) and firewalls and allows authentication by certificate, pre-shared key or username and password. OpenVPN works well through proxy servers and can run over TCP and UDP transports. Support for OpenVPN is available on several operating systems, including Windows®, Linux, Mac OS®, Solaris, OpenBSD, FreeBSD, NetBSD and QNX.

Configuring an Open VPN server

From the menu at the top of the screen, click **Networking** and from the VPN section on the left, click **OpenVPN**. A list of configured OpenVPN VPN connections is displayed.

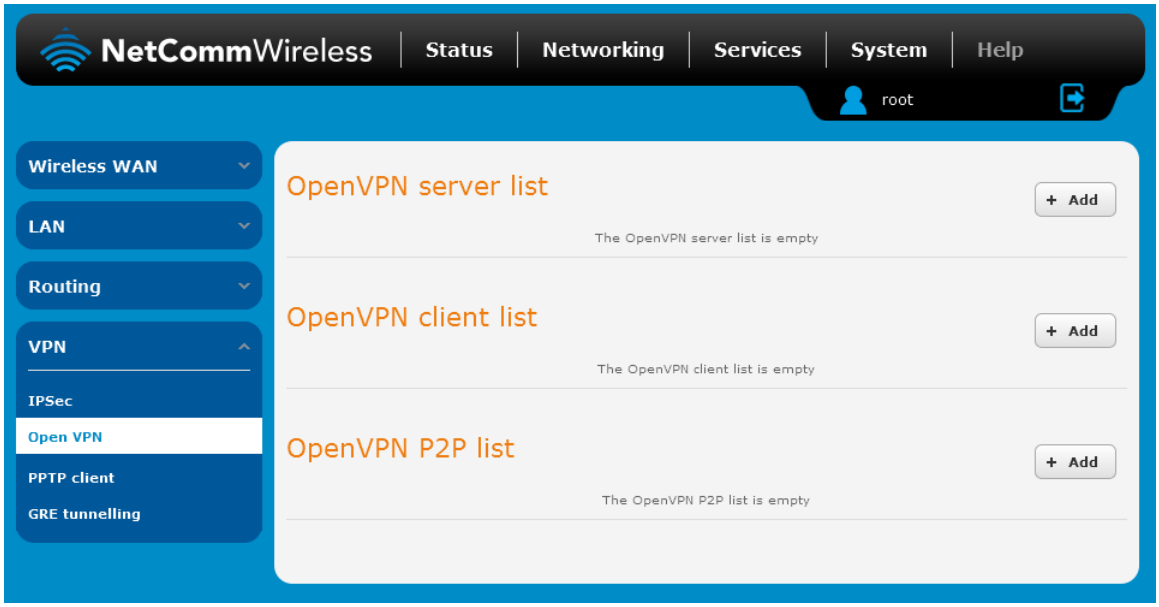


Figure 57 - OpenVPN VPN List

Click the **+Add** button for the type of OpenVPN server/client you would like to configure.

OpenVPN server

To configure an OpenVPN Server:

1. Click the **OpenVPN profile** toggle key to switch it to the **ON** position.
2. In the **Profile Name** field, type a name for the OpenVPN server profile you are creating.
3. Use the **Type** drop down list to select the interface type for the OpenVPN Server. The **TAP** virtual interface is used to transport IP, non-IP or IPv6 traffic. It simulates a data link layer device (i.e. bridge) and operates with layer 2 frames such as Ethernet frames. The **TUN** virtual interface transports IP traffic only. It simulates a network layer device (i.e. router) and operates with layer 3 packets.
4. Use the **Server** port field to select a port number and then use the drop down list to select a packet type to use for your OpenVPN Server. The default OpenVPN port is 1194 and default packet type is UDP.
5. In the **VPN network address** and **VPN network subnet mask** fields, enter the IP address and network subnet mask to assign to your VPN. This is ideally an internal IP address which differs from your existing address scheme.
6. Next to Diffie-Hellman parameters, select the number of bits to use and then click the **Generate** button. This will create an encryption key to secure your OpenVPN connection.
7. Under Server Certificates, enter the required details. All fields must be completed. The **Country** field must consist of two characters only. When the details have been entered, click the **Generate CA certificate** button to generate the Certificate Authority (CA) certificate based on this information.
8. Under the **Server certificates** section, select the **Authentication type** that you would like to use for the OpenVPN Server.

Note: The time required to generate Diffie-Hellman parameters varies based on the number of bits selected. For example, if 1024 bits is selected, the router can take approximately 1 hour to generate the parameters. Please be patient.

Certificate authentication

In the Certificate Management section, enter the required details to create a client certificate. All fields are required. When you have finished entering the details, click the **Generate** button.

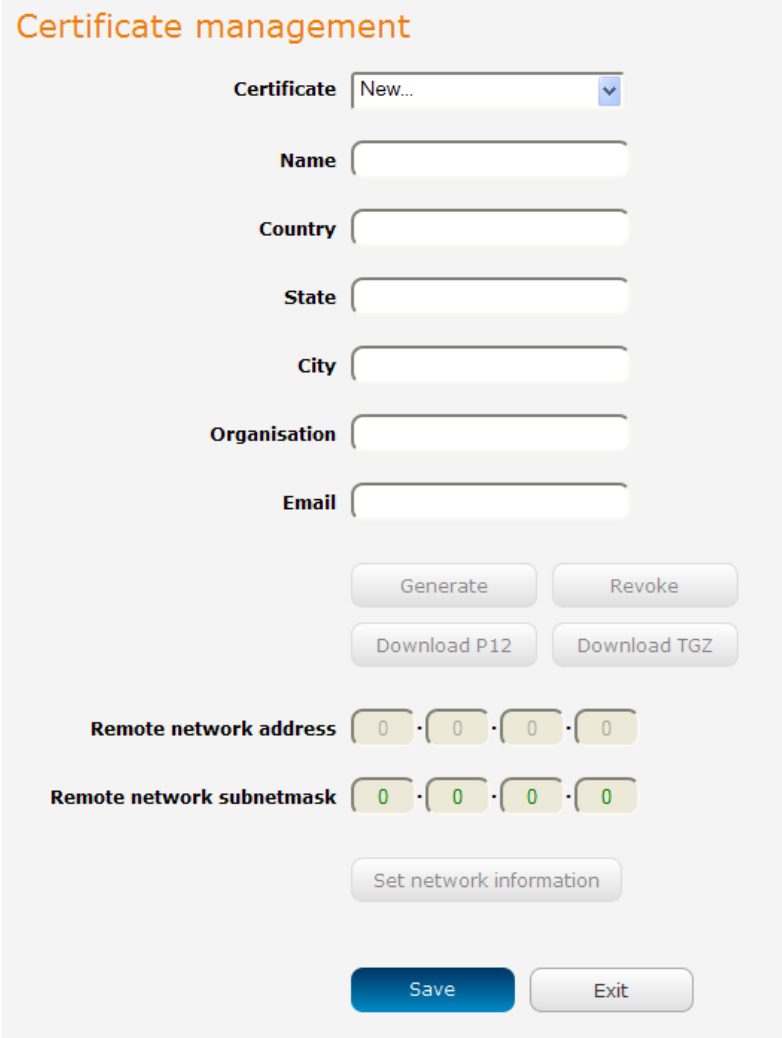


Figure 58 - OpenVPN server configuration – Certificate management

When it is done, you can click the **Download P12** button or the **Download TGZ** button to save the certificate file depending on which format you would like. If for some reason the integrity of your network has been compromised, you can return to this screen and use the Certificate drop down list to select the certificate and then press the **Revoke** button to disable it.

Optional: To inform the OpenVPN server of the network address scheme of the currently selected certificate, enter the network address and network subnet mask in the respective fields and click the **Set network information** button. If you do not enter the remote subnet here, any packet requests from the server to the client will not be received by the client network because it is not aware of the remote client's subnet.

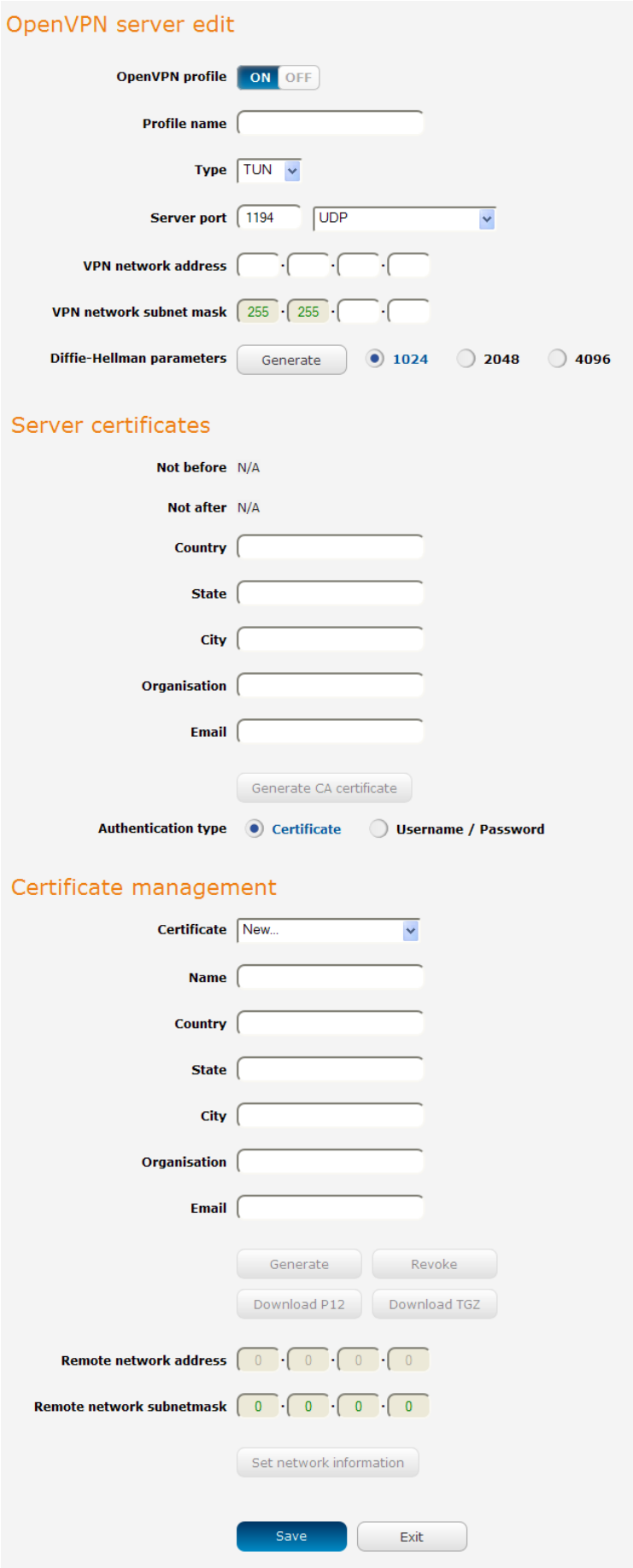


Figure 59 – OpenVPN server profile settings

Username / Password authentication

In the Username/Password section, enter the username and password you would like to use for authentication on the OpenVPN Server. Click the **Download CA TGZ** button or the **Download CA certificate** button to save the certificate file depending on the certificate format you require. This file will need to be provided to the client.

Note: If you wish to have more than one client connect to this OpenVPN server, you must use Certificate authentication mode as Username/Password only allows for a single client connection.

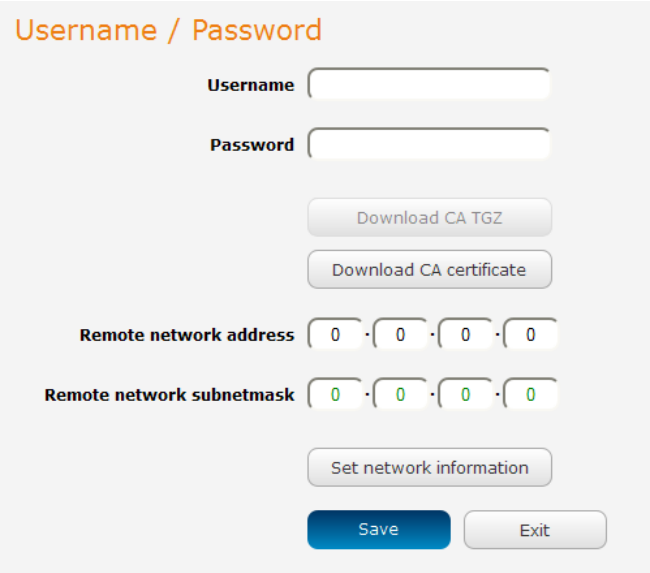


Figure 60 - OpenVPN Server – Username / Password section

Optional: To inform the OpenVPN server of the network address scheme of the currently selected certificate, enter the network address and network subnet mask in the respective fields and click the **Set Network Information** button. If you do not enter the remote subnet here, any packet requests from the server to the client will not be received by the client network because it is not aware of the remote client's subnet.

When you have finished entering all the required information, click **Save** to finish configuring the OpenVPN server.

Configuring an OpenVPN client

1. Click the **OpenVPN profile** toggle key to switch it to the **ON** position.
2. In the **Profile name** field, type a name for the OpenVPN client profile you are creating.
3. In the **Server IP** address field, type the WAN IP address of the OpenVPN server.
4. Use the **Type** drop down list to select the interface type for the OpenVPN Server. The **TAP** virtual interface is used to transport IP, non-IP or IPv6 traffic. It simulates a data link layer device (i.e. bridge) and operates with layer 2 frames such as Ethernet frames. The **TUN** virtual interface transports IP traffic only. It simulates a network layer device (i.e. router) and operates with layer 3 packets.
5. Use the **Server** port field to select a port number and then use the drop down list to select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.
6. If the **Default gateway** option is applied on the OpenVPN client page, the OpenVPN server will enable connections to be made to other client networks connected to it. If it is not selected, the OpenVPN connection allows for secure communication links between this router and the remote OpenVPN server only.
7. Use the **Authentication type** options to select the Authentication type that you would like to use for the OpenVPN client.

Certificate authentication

In the Certificate upload section at the bottom of the screen, click the **Browse** button and locate the certificate file you downloaded when you configured the OpenVPN server. When it has been selected, click the **Upload** button to send it to the router.

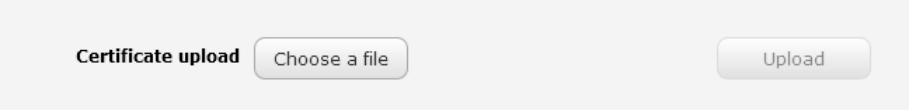


Figure 61 - OpenVPN client - Certificate upload

Username / Password authentication

Enter the username and password to authenticate with the OpenVPN server.

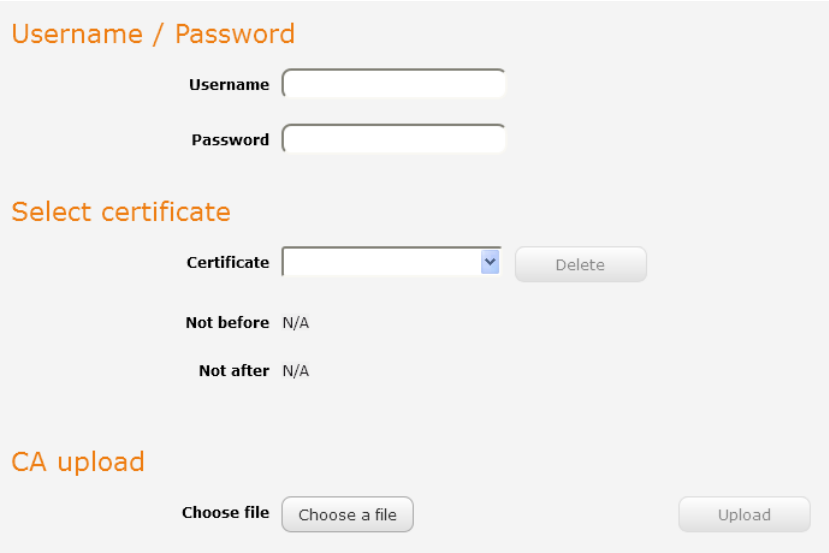


Figure 62 - OpenVPN Client - Username/Password section

Use the **Browse** button to locate the CA certificate file you saved from the OpenVPN Server and then press the **Upload** button to send it to the router.

Click the **Save** button to complete the OpenVPN Client configuration.

Certicate and Username / Password

This mode allows you to use both a certificate and username / password for authentication.

Configuring an OpenVPN P2P connection

To configure an OpenVPN peer-to-peer connection:

1. Set the **OpenVPN** profile toggle key to switch it to the **ON** position.
2. In the **Profile name** field, type a name for the OpenVPN P2P profile you are creating.
3. On the router designated as the master, leave the **Server IP address** field empty. On the router designated as the slave, enter the **WAN IP address** of the master.

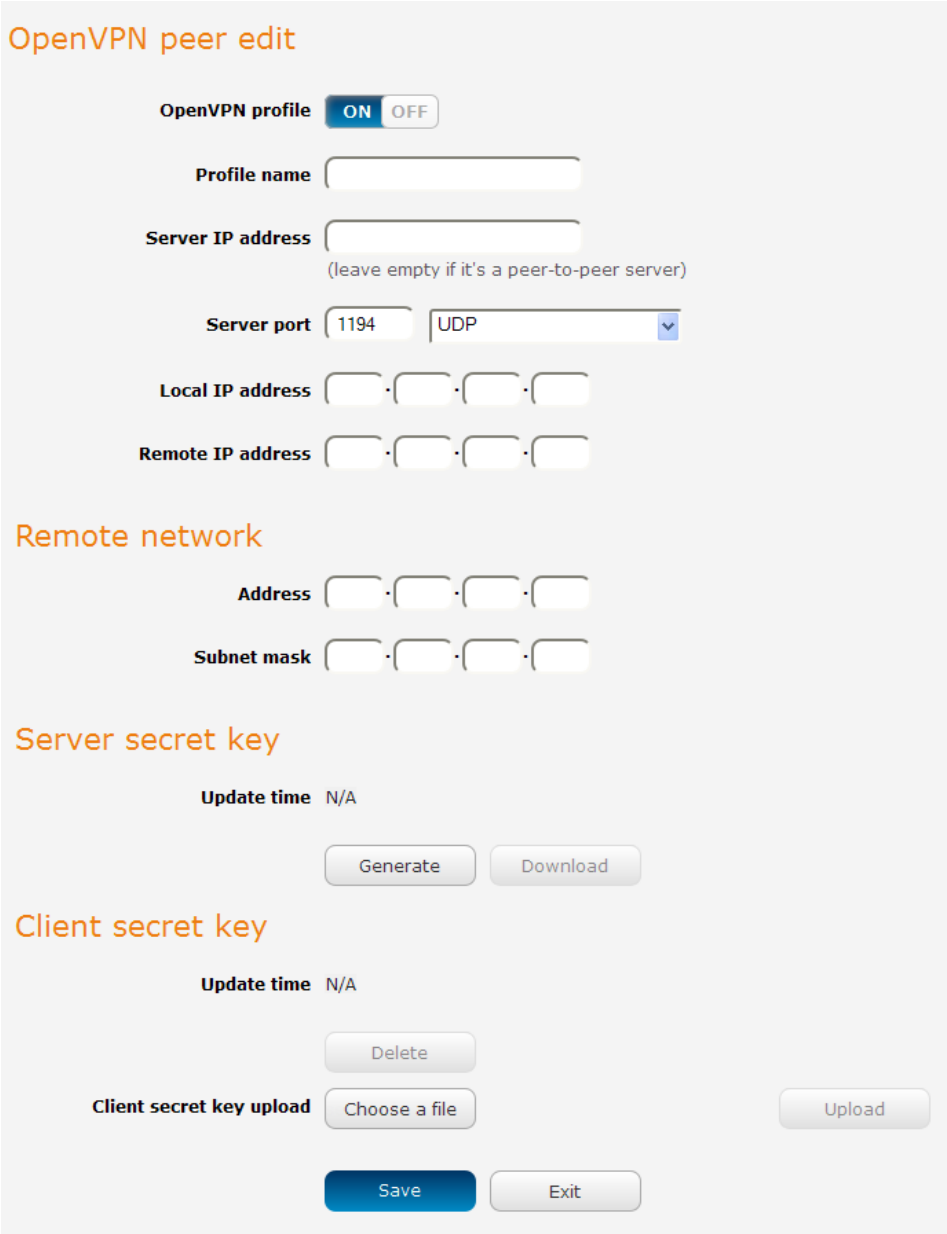


Figure 63 - OpenVPN P2P mode settings

4. Use the **Server** port field to select a port number and then use the drop down list to select a packet type to use for the OpenVPN server. The default OpenVPN port is 1194 and default packet type is UDP.
5. In the **Local IP Address** and **Remote IP Address** fields, enter the respective local and remote IP addresses to use for the OpenVPN tunnel. The slave should have the reverse settings of the master.
6. Under the Remote network section, enter the network **Address** and network **Subnet mask**. The Network Address and Network Mask fields inform the Master node of the LAN address scheme of the slave.
7. Press the **Generate** button to create a secret key to be shared with the slave. When the timestamp appears, you can click the **Download** button to save the file to exchange with the other router.
8. When you have saved the secret key file on each router, use the **Browse** button to locate the secret key file for the master and then press the **Upload** button to send it to the slave. Perform the same for the other router, uploading the slave's secret key file to master.
9. When they are uploaded click the **Save** button to complete the peer-to-peer OpenVPN configuration.

PPTP client

The Point-to-Point Tunnelling Protocol (PPTP) is a method for implementing virtual private networks using a TCP and GRE tunnel to encapsulate PPP packets. PPTP operates on Layer 2 of the OSI model and is included on Windows computers.

Configuring the PPTP client

To configure the PPTP client:

1. From the menu bar at the top of the screen, click **Networking** and then from the **VPN** section on the left side of the screen, click **PPTP client**. The PPTP client list is displayed.

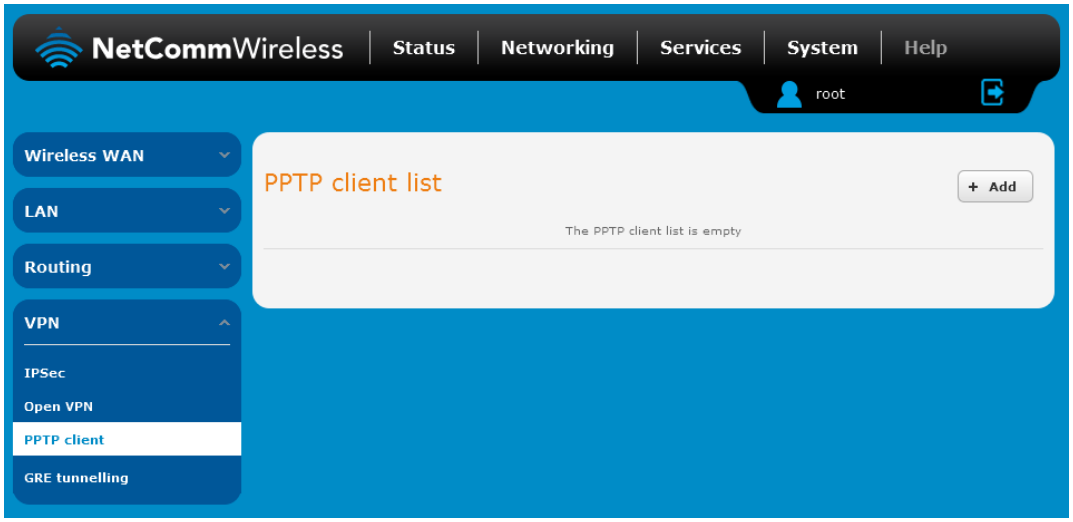


Figure 64 - PPTP client list

2. Click the **+Add** button to begin configuring a new PPTP client profile. The PPTP client edit screen is displayed.

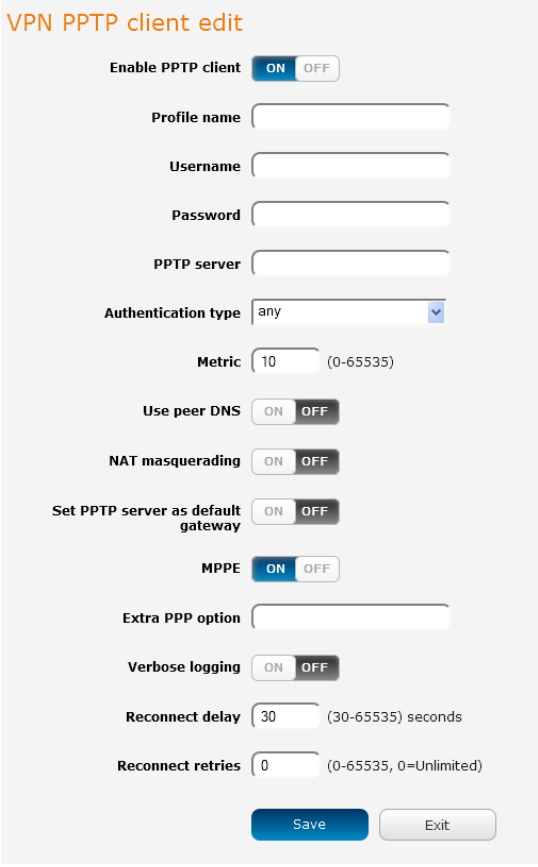


Figure 65 - VPN PPTP client edit

3. Click the **Enable PPTP client** toggle key to switch it to the **ON** position.
4. In the **Profile name list,** enter a profile name for the tunnel. This may be anything you like and is used to identify the tunnel on the router.
5. Use the **Username** and **Password** fields to enter the username and password for the PPTP account.
6. In the **PPTP server address** field, enter the IP address of the PPTP server.
7. From the **Authentication type** drop down list, select the Authentication type used on the server. If you do not know the authentication method used, select **any** and the router will attempt to determine the correct authentication type for you. There are 5 authentication types you can choose from:
   - CHAP – uses a three way handshake to authenticate the identity of a client.
   - MS-CHAP v1 – This is the Microsoft implementation of the Challenge Handshake Authentication Protocol for which support was dropped in Windows® Vista.
   - MS-CHAP v2 - This is the Microsoft implementation of the Challenge Handshake Authentication Protocol which was introduced in Windows® NT 4.0 and is still supported today.
   - PAP – The Password Authentication Protocol uses a password as a means of authentication and as such, is commonly supported. PAP is not recommended because it transmits passwords unencrypted and is not secure.
   - EAP – Extensible Authentication Protocol. An Authentication protocol commonly used in wireless networks.
8. The **metric** value helps the router to prioritise routes and must be a number between 0 and 65535. The default value is 30 and should not be modified unless you are aware of the effect your changes will have.
9. The **Use peer DNS** option allows you to select whether the remote clients will use the Domain Name Server of the PPTP server. Click the toggle key to set this to ON or OFF as required.
10. **NAT masquerading** allows the router to modify the packets sent and received to inform remote computers on the internet that packets originating from a machine behind the router actually originated from the WAN IP address of the router's internal NAT IP address. Click the toggle key to switch this to the ON position if you want to use this feature.
11. Set **default route to PPTP** sets all outbound data packets to go out through the PPTP tunnel. Click the toggle key to switch this to the ON position if you want to use this feature.
12. Select whether to use **MPPE**. MPPE stands for Microsoft Point-to-Point Encryption and is used to encrypt data across the virtual private network. The **MPPE** option is enabled by default.
13. The **Verbose logging** option sets the router to output detailed logs regarding the PPTP connection in the **System Log** section of the router interface.
14. The **Reconnect delay** is the time in seconds that the router will wait before attempting to connect to the PPTP server in the event that the connection is broken. The minimum time to wait is 30 seconds so as to not flood the PPTP server with connection requests, while the maximum time to wait is 65335 seconds.
15. The **Reconnect retries** is the number of connection attempts that the router will make in the event that the PPTP connection goes down. If set to 0, the router will retry the connection indefinitely, otherwise the maximum number of times to retry cannot be greater than 65335.
16. Click the **Save** button to save the changes. The VPN will attempt to connect after your click Save. Click the **Status** button at the top left of the interface to return to the status window and monitor the VPN's connection state.

GRE tunnelling

The Generic Route Encapsulation (GRE) protocol is used in addition to Point-to-Point Tunnelling Protocol (PPTP) to create VPNs (virtual private networks) between clients and servers or between clients only. Once a PPTP control session establishes the VPN tunnel GRE is used to securely encapsulate the data or payload.

Configuring GRE tunnelling

To configure GRE tunnelling:

1. From the menu bar at the top of the screen, click **Networking** and then from the **VPN** section on the left side of the screen, click **GRE**. The GRE client list is displayed.

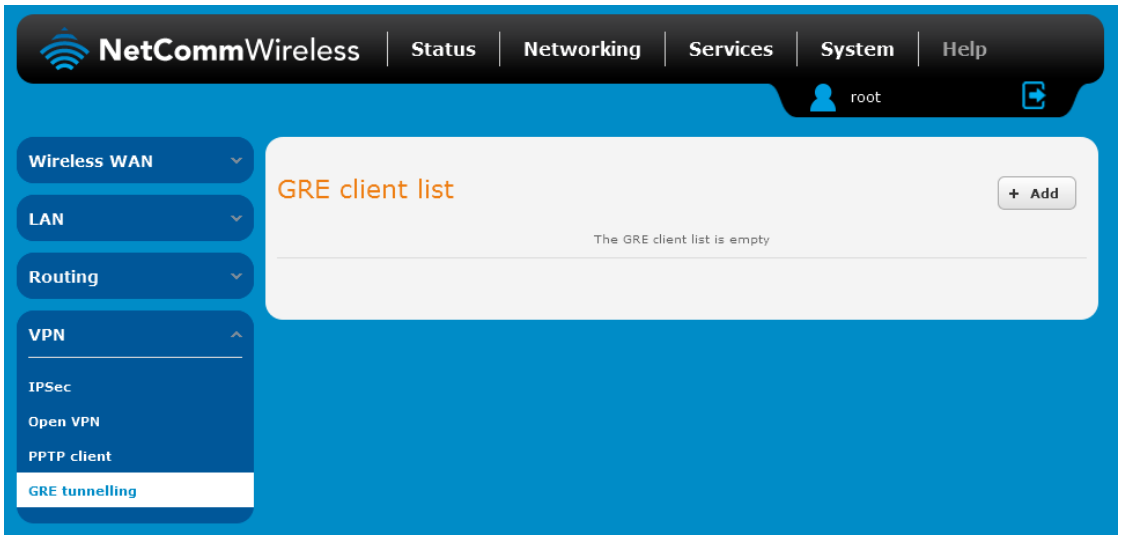


Figure 66 - GRE client list

2. Click the **+Add** button to begin configuring a new GRE tunnelling client profile. The GRE Client Edit screen is displayed.

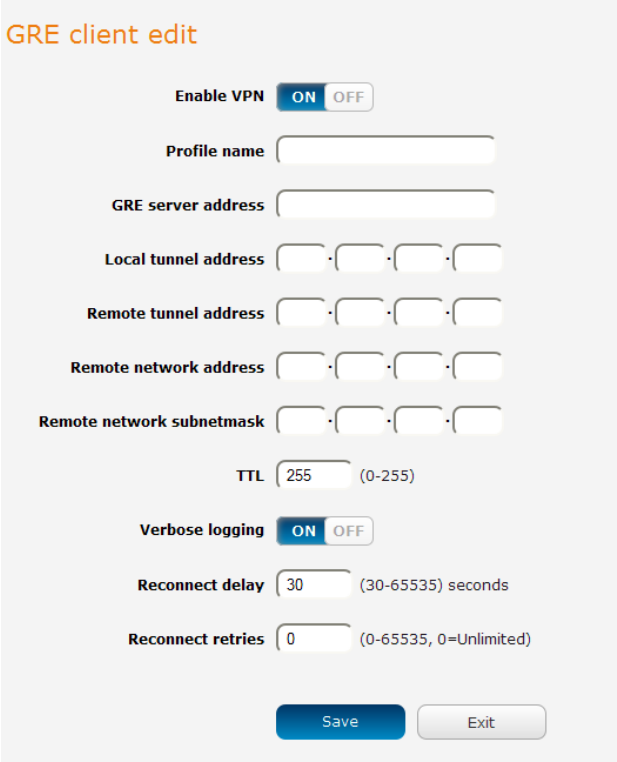


Figure 67 – GRE client edit

3. Click the **Enable GRE Tunnel** toggle key to switch it to the **ON** position.

4. In the **Profile name**, enter a profile name for the tunnel. This may be anything you like and is used to identify the tunnel on the router.
5. In the **GRE Server Address** field, enter the IP address of the GRE server.
6. In the **Local Tunnel Address** field, enter the IP address you want to assign the tunnel locally.
7. In the **Remote Tunnel Address** field, enter the IP address you want to assign to the remote tunnel.
8. In the **Remote Network Address** field, enter the IP address scheme of the remote network.
9. In the **Remote Network/Mask** field, enter the subnet mask of the remote network.
10. The **TTL** (Time To Live) field is an 8-bit field used to remove an undeliverable data packet from a network to avoid unnecessary network traffic across the internet. The default value of 255 is the upper limit on the time that an IP datagram can exist. The value is reduced by at least one for each hop the data packet takes to the next router on the route to the datagram's destination. If the TTL field reaches zero before the datagram arrives at its destination the data packet is discarded and an error message is sent back to the sender.
11. The **Verbose logging** option sets the router to output detailed logs regarding the GRE tunnel in the **System Log** section of the router interface.
12. The **Reconnect delay** is the time in seconds that the router will wait before attempting to connect to the GRE server in the event that the connection is broken. The minimum time to wait is 30 seconds so as to not flood the GRE server with connection requests, while the maximum time to wait is 65335 seconds.
13. The **Reconnect retries** is the number of connection attempts that the router will make in the event that the GRE connection goes down. If set to 0, the router will retry the connection indefinitely, otherwise the maximum number of times to retry cannot be greater than 65335.
14. Click the **Save** button to save the changes. The VPN will attempt to connect after your click Save. Click the **Status** button at the top left of the interface to return to the status window and monitor the VPN's connection state.

Services

Dynamic DNS

The DDNS page is used to configure the Dynamic DNS feature of the router. A number of Dynamic DNS hosts are available from which to select.

Figure 68 – Dynamic DNS settings

Dynamic DNS provides a method for the router to update an external name server with the current WAN IP address.

To configure dynamic DNS:

1. Click the **DDNS configuration** toggle key to switch it to the ON position.
2. From the **Dynamic DNS** drop down list, select the Dynamic DNS service that you wish to use. The available DDNS services available are:
   - www.dhs.org
   - www.dyndns.org
   - www.dyns.cx
   - www.easydns.com
   - www.justlinux.com
   - www.ods.org
   - www.tzo.com
   - www.zoneedit.com
3. In the **Username** and **Password** fields, enter the logon credentials for your DDNS account. Enter the password for the account again in the **Verify password** field.
4. Click the **Save** button to save the DDNS configuration settings.

Network time (NTP)

The NTP (Network Time Protocol) settings page allows you to configure the NWL-15 router to synchronize its internal clock with a global Internet Time server and specify the time zone for the location of the router. This provides an accurate timekeeping function for features such as System Log entries and Firewall settings where the current system time is displayed and recorded.

Any NTP server available publicly on the internet may be used. The default NTP server is 0.netcomm.pool.ntp.org.

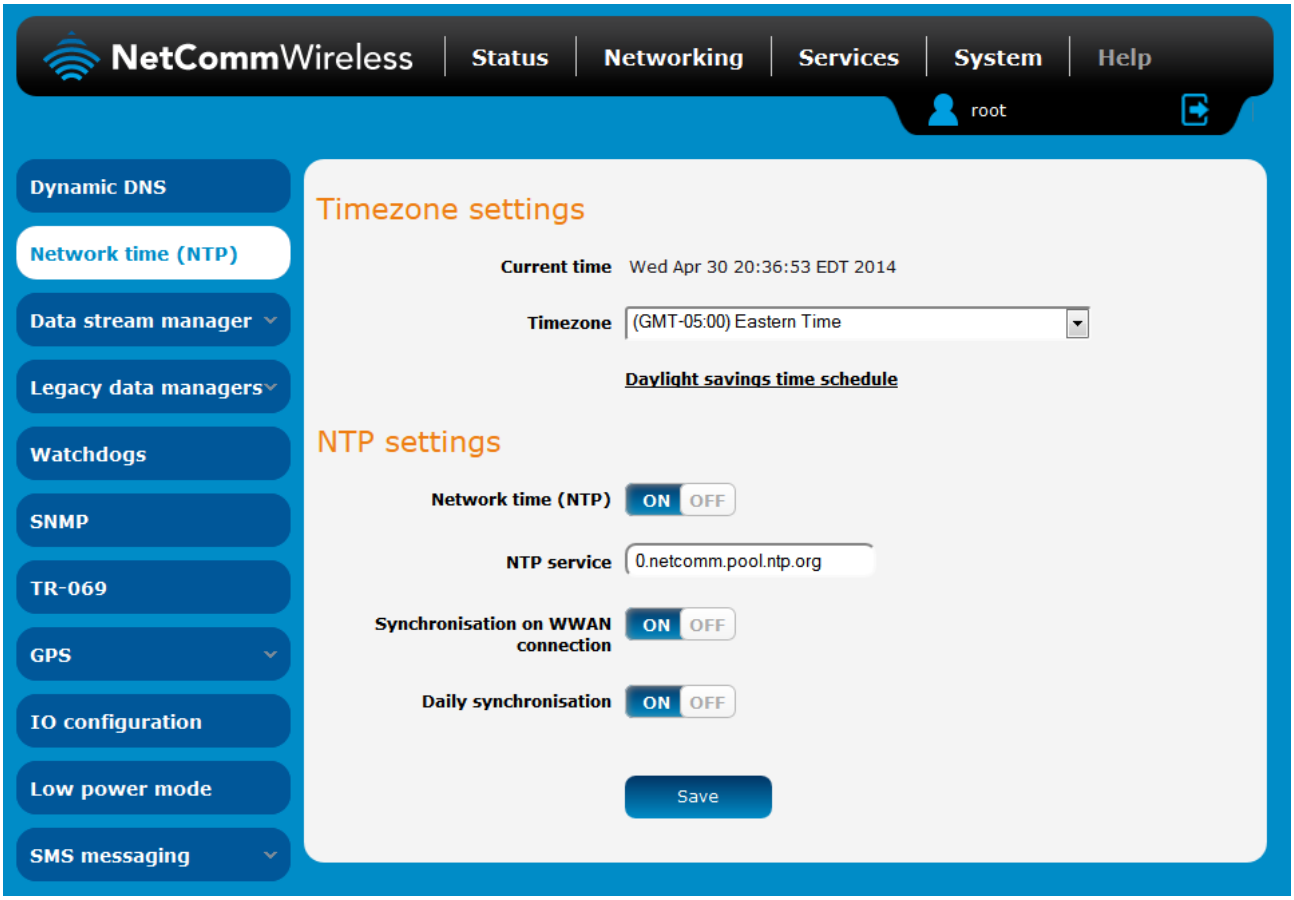


Figure 69 - NTP settings

Configuring Timezone settings

To configure time zone settings:

1. The **Current time** field shows the time and date configured on the router. If this is not accurate, use the **Time zone** drop down list to select the correct time zone for the router. If the selected zone observes daylight savings time, a **Daylight savings time schedule** link appears below the drop down list. Click the link to see the start and end times for daylight savings.
2. When you have selected the correct time zone, click the **Save** button to save the settings.

Configuring NTP settings

To configure NTP settings:

1. Click the **Network time (NTP)** toggle key to switch it to the **ON** position.
2. In the **NTP service** field, enter the address of the NTP server you wish to use.
3. The **Synchronization on WWAN connection** toggle key enables or disables the router from performing a synchronization of the time each time a mobile broadband connection is established.
4. The **Daily synchronization** toggle key enables or disables the router from performing a synchronization of the time each day.
5. When you have finished configuring NTP settings, click the **Save** button to save the settings.

Data stream manager

The data stream manager provides you with the ability to create mappings between two endpoints on the router. These endpoints may be physical or virtual, for example, the built-in serial port could be configured as an endpoint or you could configure a TCP Server as an endpoint. You can then configure a virtual data tunnel or "stream" between the endpoints.

The data stream manager provides a wide range of possibilities and expands upon simple PAD functionality to include the forwarding and translation of data between any of the endpoints. For example, you could send the GPS data received by the module (in NMEA format) through a serial port (by means of a USB-to-Serial cable). In each case, the logical flow of data is from Endpoint A to Endpoint B.

Customers interested in developing their own applications to create custom endpoints and streams can contact NetComm Wireless about our Software Development Kit.

Endpoints

The first thing to be done in order to create a data stream is to define the endpoints. There are 6 types of endpoint that may be configured:

- Serial port (generic)
- TCP Server
- TCP Client
- UDP Server
- UDP Client
- GPS Data (for devices with GPS receiver)

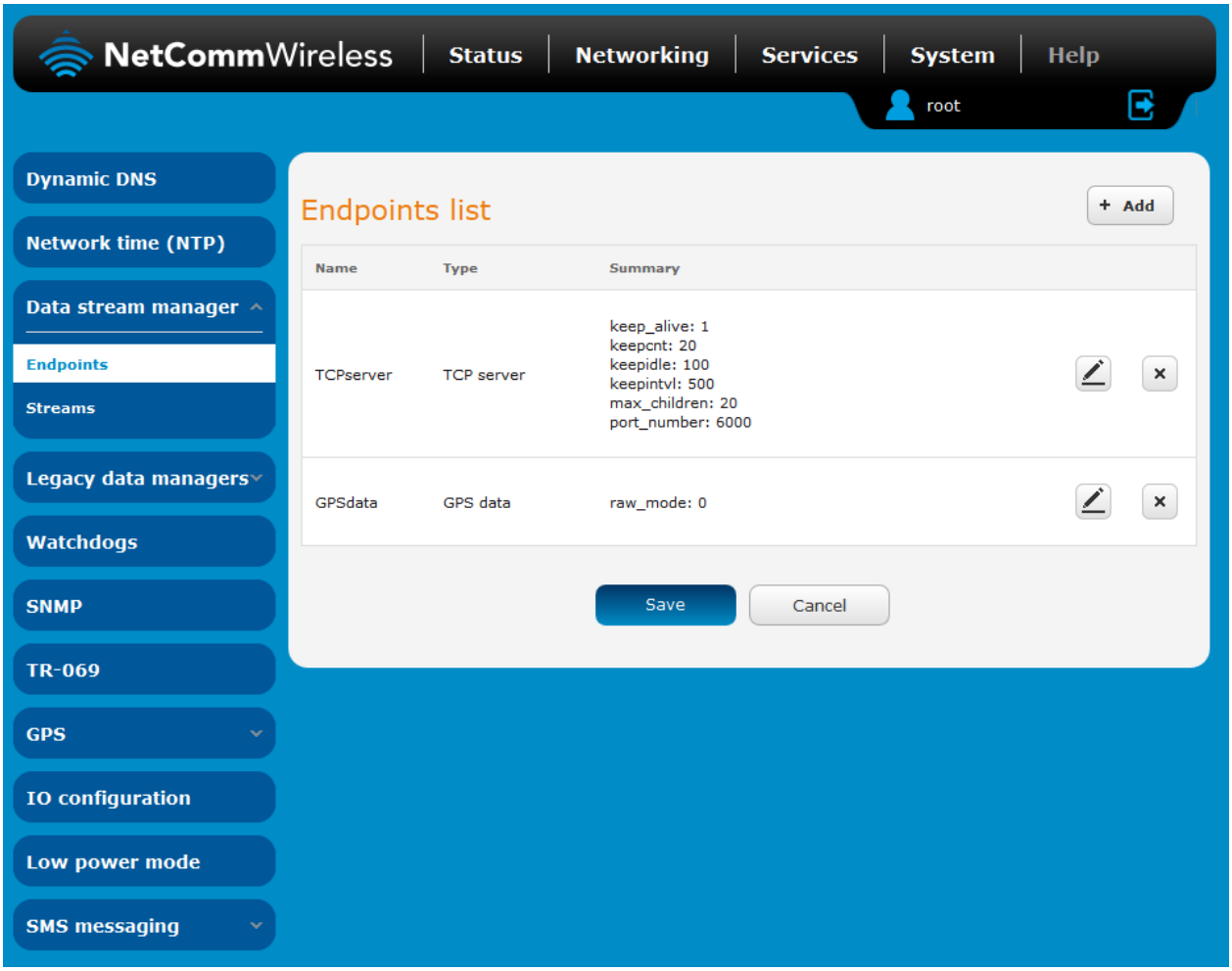


Figure 70 - Endpoints list

To create an endpoint:

1. Click the **+Add** button on the right side of the page. A pop-up window appears.

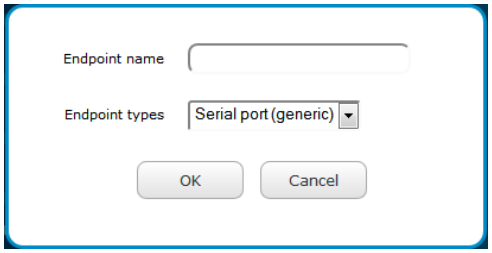


Figure 71 - Creating an endpoint

2. In the **Endpoint name** field, type a name for this endpoint. The name can contain alphanumeric characters only i.e. A-Z, a-z, 0-9.
3. Use the **Endpoint types** drop down list to select the type of endpoint to configure.

   Serial port (generic): This creates a generic serial port as an endpoint defaulting to the commonly used settings as shown below.

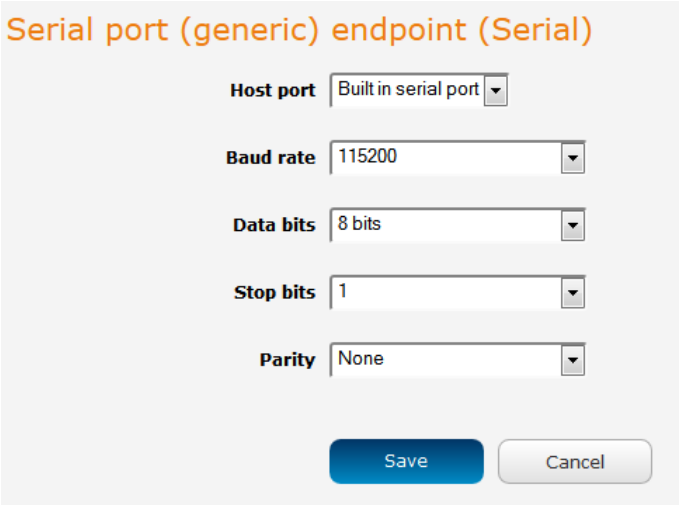


Figure 72 - Serial port (generic) endpoint configuration

TCP server: This creates a TCP server endpoint with the following options available.

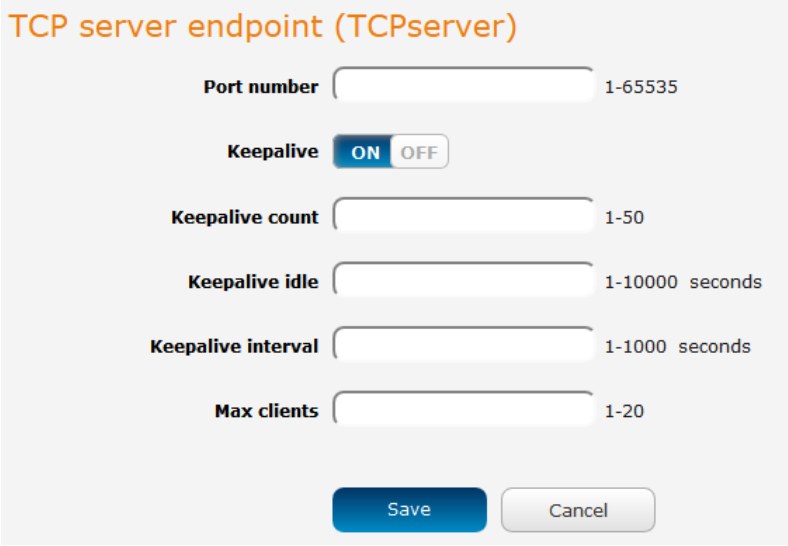


Figure 73 - TCP server endpoint configuration

TCP client: This creates a TCP client endpoint with the following options available. The retry timeout period specifies the number of seconds to wait between attempts to re-establish a connection in the event that it is lost. The client will attempt re-connection indefinitely every Retry timeout interval.

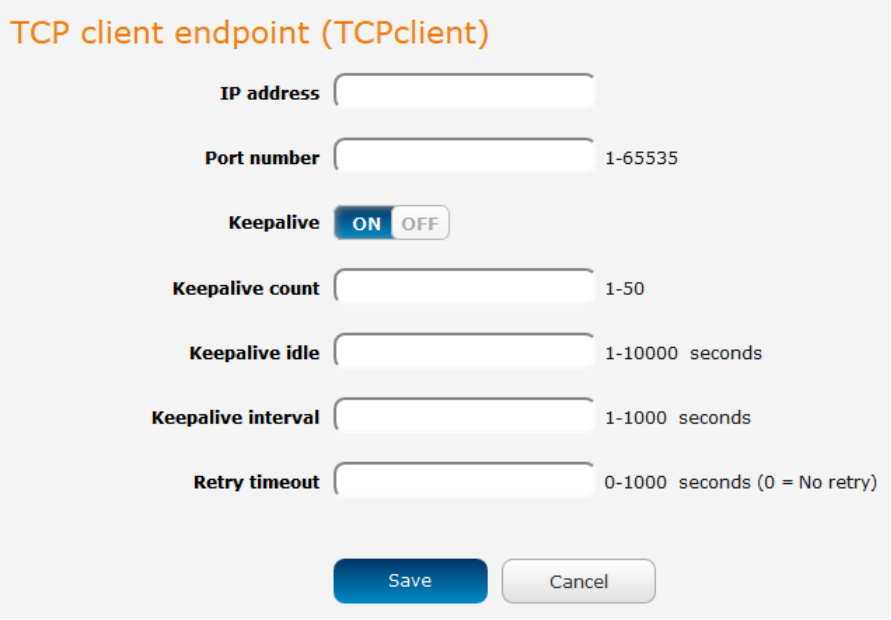


Figure 74 - TCP client endpoint configuration

UDP server: This creates a UDP server endpoint with the following options available.

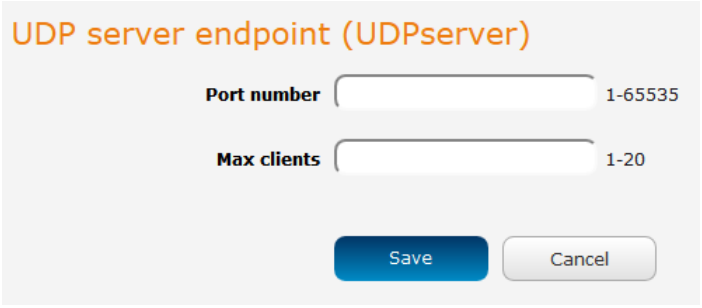


Figure 75 - UDP server endpoint configuration

UDP client: This creates a UDP client endpoint with the following options available. The retry timeout period specifies the number of seconds to wait between attempts to re-establish a connection in the event that it is lost. The client will attempt re-connection indefinitely every Retry timeout interval.

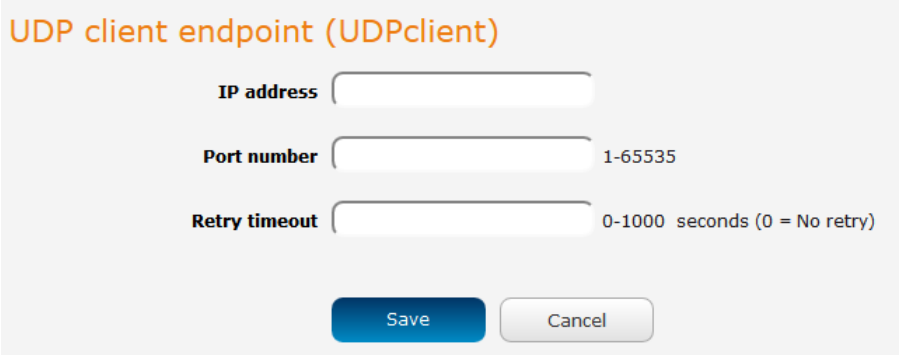


Figure 76 - UDP client endpoint configuration

GPS data: This creates a GPS data endpoint.

Figure 77 - GPS data endpoint configuration

4. Click the **OK** button. The router displays a screen with configuration options for your chosen endpoint type.
5. Enter the options for your endpoint as required.
6. Click the **Save** button. The Endpoints list is displayed with the newly created endpoint listed and a summary of the settings your configured.

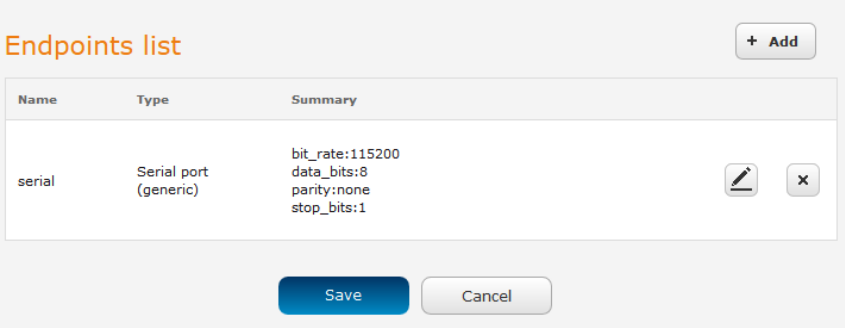


Figure 78 - Endpoints list

Streams

When you have created the required endpoints, you can then proceed to set up a data stream. A data stream sends data from one endpoint to another, performing any transformation of the data as required. When a stream is added, an underlying process on the router checks the validity of the stream, checking for conflicts and illogical configurations.

Notes on data stream operation:

- When any changes to the Data stream manager configuration are detected, all data streams are stopped and restarted as per the new configuration.
- Multiple Modbus clients cannot connect simultaneously to Modbus serial slaves connected to the router.

Every stream requires two endpoints, Endpoint A and Endpoint B. In all cases, the flow of data is from Endpoint A to Endpoint B.

To create a new stream:

7. Click the **+Add** button on the right side of the page.

Figure 79 - Data stream list

The Edit data stream page is displayed.

8. In the **Data stream name** field, enter a name for the Data stream.
9. Under Endpoint A, use the **Endpoint name** drop down list to select one of the endpoints you created previously. This endpoint should be the starting point of the stream. Use the **Mode** drop down list to select the mode of operation of the endpoint. The mode can be thought of as a transformation of the data as it leaves this endpoint. For example, if Endpoint A type is Serial port (generic), the Mode can be set to various Modbus server and client types. This means that upon arrival at Endpoint A, the data will be transformed into the chosen Modbus format, ready to be sent to Endpoint B.

10. Under Endpoint B, use the **Endpoint name** drop down list to select one of the endpoints you created previously. This endpoint should be the destination of the stream. The screenshot below shows a configuration sending GPS data out of the built-in serial port. Use the **Mode** drop down list to select the mode of operation of the endpoint. The mode can be thought of as a transformation of the data as it arrives at this endpoint.

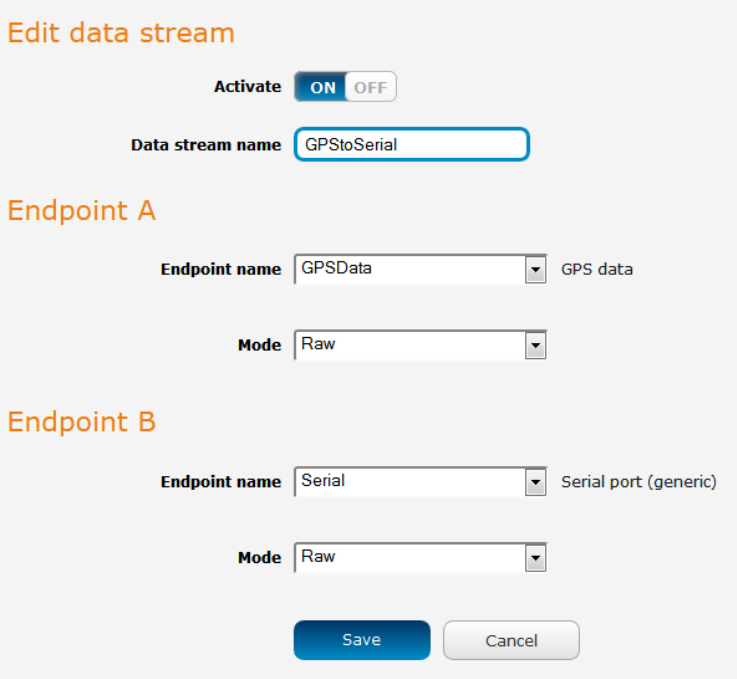


Figure 80 - Edit data stream

11. Click the **Save** button. The new stream appears in the Data stream list.

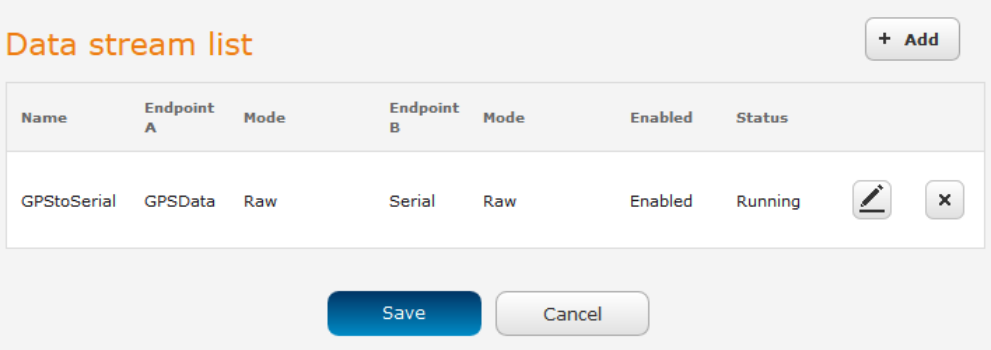


Figure 81 - Data stream list

.

Legacy data managers

Modem emulator

Modem emulator allows you to connect legacy equipment such as an RTU or PLC to the serial port of the router in place of a traditional dial-up modem. The NWL-15 router emulates the dial-up modem's behavior and passes the serial data over the IP network.

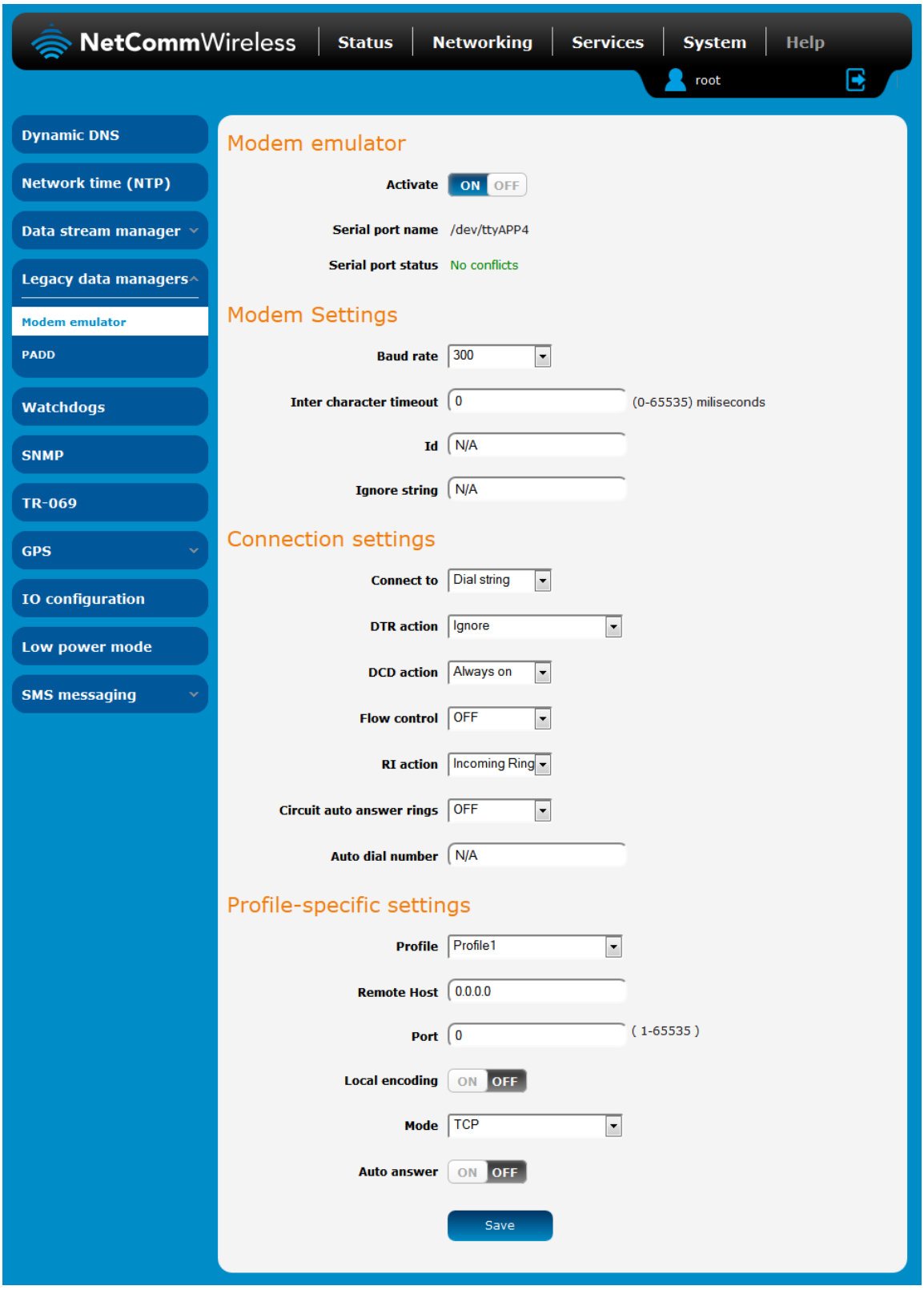


Figure 82 - Modem emulator

ITEM	DESCRIPTION
Modem emulator	
Activate	Turns on or off the modem emulator function of the router.
Serial port name	The device name of the serial port.
Serial port status	The configuration status of the serial port. This will display whether there are any conflicts with the serial port preventing modem emulator from working properly.
Modem settings	
Baud rate	The serial (V.24) port baud rate. By default the serial line format is 8 data bits, No parity, 1 Stop bit. Refer to the AT (V.250) AT Command Manual if you need to change the serial line format.
Inter character timeout	The Modem emulator buffers any bytes received from the serial port until either 512 bytes have been received or no bytes have been received for "Inter Character Timeout" milliseconds, it will then send any bytes in the buffer to the remote host.
Id	When the ID field is not blank (empty) the defined ID will be sent to the remote host as follows: For UDP the 1st <n> bytes of each datagram sent will be set to the contents of the ID field, data follows immediately after the ID for TCP the ID is transmitted once immediately after the connection is established
Ignore string	When the "Ignore String" field is not blank (empty) the router will strip any character sequence that matches the "Ignore String" from the data stream received from the serial port.
Connection settings	
Connect to	Determines how the router behaves when it receives an "ATD" command on the serial port. • Profile - Connect using "Data Connection Profile" • Circuit - Establish a circuit switched data connection • Packet - Connect to cellular packet network in PPP pass through mode • DialString - Examine the dialed digits and connect to Profile, Circuit or Packet as appropriate
DTR action	Determines how the router responds to change of state of the serial port DTR line • Ignore - Take no action • Command - High to Low transition of DTR causes the router to enter command mode (does not end call). • Hangup - High to Low transition of DTR causes the router to end call and enter command mode. • High AutoDial - Low to High transition of DTR causes the router to dial the Auto Dial Number, High to Low transition of DTR causes the router to end call and enter command mode. • Low AutoDial - High to Low transition of DTR causes the router to dial the Auto Dial Number, Low to High transition of DTR causes the router to end call and enter command mode. • Low Pass To ATPort - When DTR is low pass all AT commands directly to internal cellular data engine.
Flow control	• Off - Serial port flow control off • Hardware - Serial port uses RTS/CTS flow control
RI action	Determines how the router controls the state of the serial port RI line • Always On - RI is always on • Incoming Ring - RI is on when an incoming connection request is received. • Always Off - RI is always off
Circuit auto answer rings	Sets the number of incoming rings after which the router will answer incoming circuit switched data calls.
Auto dial number	Sets the number the router will dial if DTR Auto Dial is enabled ad DTR changes state.
Profile-specific settings (these items may be configured separately for each of the 4 connection profiles)	
Profile	Choose the profile that you want to configure.
Remote Host	In client mode (router connects to host) this is the remote host to which the router will connect. In server mode (remote host connects to router) the router will only accept incoming connections from the specified host. If you specify 0.0.0.0 the router will accept incoming connections from any host.
Port	TCP/UDP port number to use
Local encoding	Refer to the AT (V.250) Command Manual for details of this parameter, this is normally disabled.
Mode	Selects the mode of operation for the chosen profile. Mode may be TCP, UDP or GMTP.
Auto answer	When enabled the router accepts incoming connections (enables server mode)

Table 16 - Modem emulator options

PADD

PAD Daemon is a tool used to encapsulate raw serial data into a TCP packet to be transported over IP to another end point. The server receiving the TCP packets unpacks the data and the original raw serial data is passed out of its serial port to the attached device, thereby creating an invisible IP network to the two serial devices.

The PAD Daemon runs as a background process which can be accessed via the web configuration interface. The PADD configuration page is located under "Services > PADD". The PADD is used usually with multiple connections or when redundant connections are needed. The PADD has two modes: the PADD TCP/IP Server mode and PADD TCP/IP Client Mode. When PADD is enabled, both the PADD server mode and PADD client mode can be run at the same time.

The PADD configuration page is shown below.

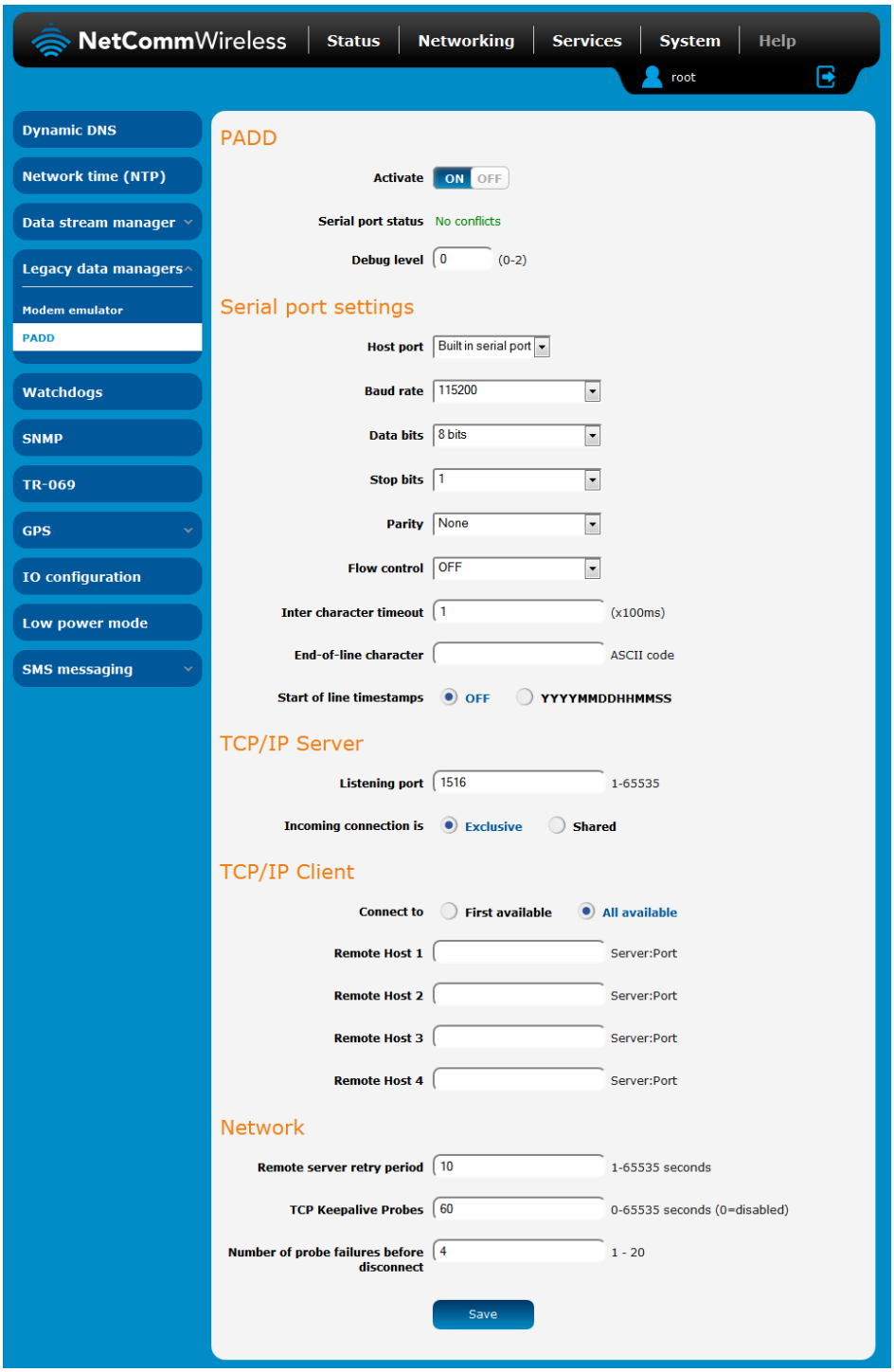


Figure 83 – PADD

A whitepaper with full Instructions on configuring PADD Mode is available at http://support.netcommwireless.com/product/m2m/nwl-15

Watchdogs

To access the Watchdogs page, click the **Services** menu item, then select the **Watchdogs** menu item on the left.

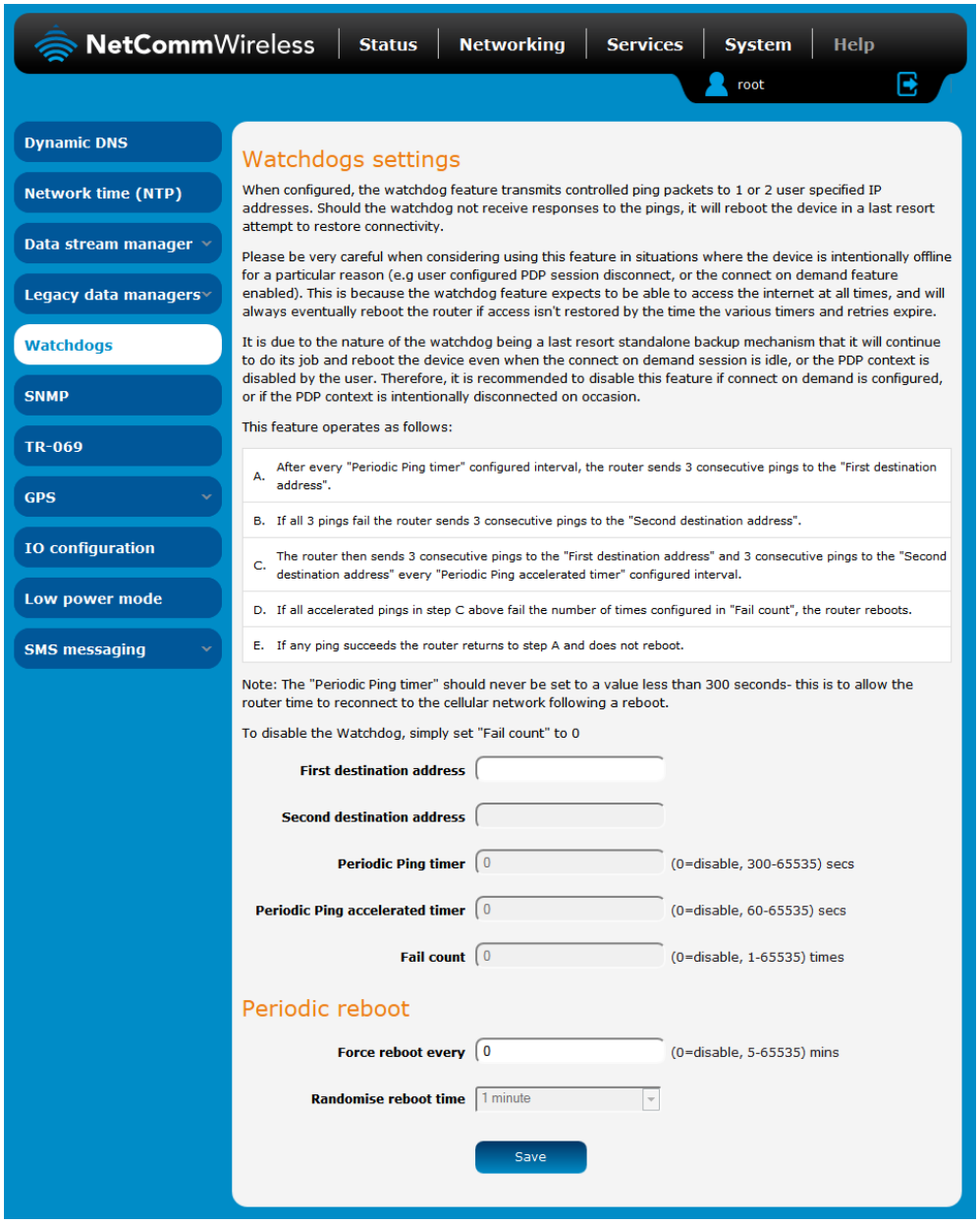

NetCommWireless
Status
Networking
Services
System
Help
root
Dynamic DNS
Network time (NTP)
Data stream manager
Legacy data managers
Watchdogs
SNMP
TR-069
GPS
IO configuration
Low power mode
SMS messaging
Watchdogs settings
When configured, the watchdog feature transmits controlled ping packets to 1 or 2 user specified IP addresses. Should the watchdog not receive responses to the pings, it will reboot the device in a last resort attempt to restore connectivity.
Please be very careful when considering using this feature in situations where the device is intentionally offline for a particular reason (e.g user configured PDP session disconnect, or the connect on demand feature enabled). This is because the watchdog feature expects to be able to access the internet at all times, and will always eventually reboot the router if access isn't restored by the time the various timers and retries expire.
It is due to the nature of the watchdog being a last resort standalone backup mechanism that it will continue to do its job and reboot the device even when the connect on demand session is idle, or the PDP context is disabled by the user. Therefore, it is recommended to disable this feature if connect on demand is configured, or if the PDP context is intentionally disconnected on occasion.
This feature operates as follows:
A. After every "Periodic Ping timer" configured interval, the router sends 3 consecutive pings to the "First destination address".
B. If all 3 pings fail the router sends 3 consecutive pings to the "Second destination address".
C. The router then sends 3 consecutive pings to the "First destination address" and 3 consecutive pings to the "Second destination address" every "Periodic Ping accelerated timer" configured interval.
D. If all accelerated pings in step C above fail the number of times configured in "Fail count", the router reboots.
E. If any ping succeeds the router returns to step A and does not reboot.
Note: The "Periodic Ping timer" should never be set to a value less than 300 seconds- this is to allow the router time to reconnect to the cellular network following a reboot.
To disable the Watchdog, simply set "Fail count" to 0
First destination address
Second destination address
Periodic Ping timer
0
(0=disable, 300-65535) secs
Periodic Ping accelerated timer
0
(0=disable, 60-65535) secs
Fail count
0
(0=disable, 1-65535) times
Periodic reboot
Force reboot every
0
(0=disable, 5-65535) mins
Randomise reboot time
1 minute
Save

Figure 84 - Watchdogs Settings

Watchdogs are features which monitor the router for anomalies and restart the router if an anomaly occurs preventing its normal operation. When configured, the watchdogs feature transmits controlled ping packets to 1 or 2 user specified IP addresses to confirm an active connection. If the watchdog does not receive responses to the pings after a specified number of failures, it will reboot the device in a last resort attempt to restore connectivity.

We recommend using caution when implementing this feature in situations where the device is intentionally offline for a particular reason, for example, when Connect on demand has been enabled. This is because the watchdog expects to be able to access the internet at all times, and will always eventually reboot the router if access isn't restored by the time the various timers expire and the fail count is reached.

It is due to the nature of the watchdog being a last resort standalone backup mechanism that it will continue to do its job and reboot the device even when the Connect on demand session is idle, or the mobile broadband connection is disabled by the user. Therefore, we recommended that you disable this feature if Connect-on-demand is configured or if the mobile broadband connection will be intentionally disconnected on occasion.

The watchdog works as follows:

1. The router sends 3 consecutive pings to the first destination address at the interval specified in the **Periodic Ping timer** field.
2. If all 3 pings to the first destination address fail, the router sends 3 consecutive pings to the second destination address at the **Periodic Ping timer** interval.
3. If all 3 pings to the second destination address fail, the router sends 3 pings to the first destination address using the **Periodic Ping accelerated timer** interval.
4. If all 3 accelerated pings to the first destination address fail, the router sends 3 pings to the second destination address at the **Periodic Ping accelerated timer** interval.
5. If all 3 accelerated pings to the second destination address fail, the router registers this as a fail and returns to step C.
6. When the number of failures reaches the number configured in the **Fail count** field, the router reboots. If any ping succeeds, the router returns to step A and does not reboot.

Note: The **Periodic Ping timer** should not be set to a value of less than 300 seconds to allow the router time to reconnect to the cellular network following a reboot.

To disable the Watchdog, set **Fail count** to 0.

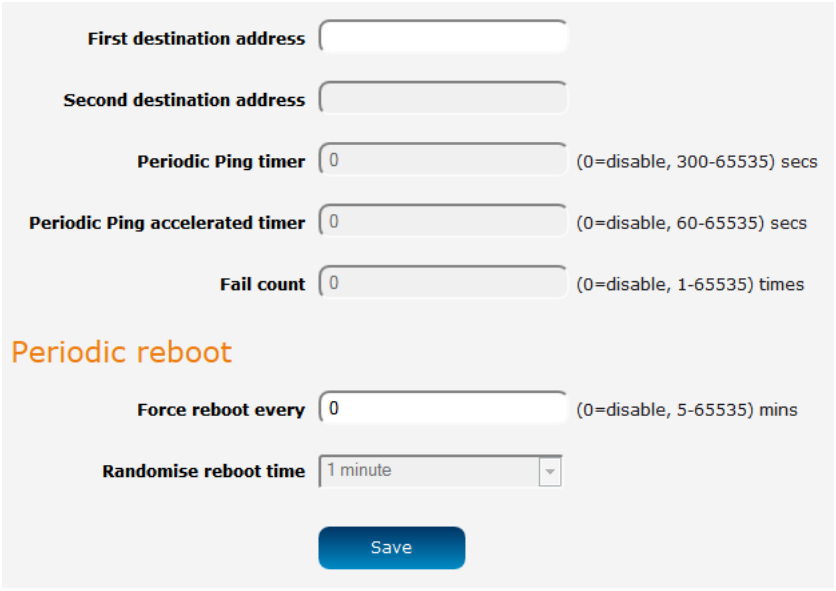


Figure 85 – Watchdog settings

Configuring Watchdog settings

The Watchdog settings configure the router to transmit controlled ping packets to 2 specified IP addresses. If the router does not receive responses to the pings, the router will reboot.

To configure the ping watchdog:

1. In the **First destination address** field, enter a website address or IP address to which the router should send the first round of ping requests.
2. In the **Second destination address** field, enter a website address or IP address to which the router should send the second round of ping requests.
3. In the **Periodic Ping timer** field, enter an integer between 300 and 65535 for the number of seconds the router should wait between ping attempts. Setting this to 0 disables the ping watchdog function.
4. In the **Periodic Ping accelerated timer** field, enter an integer between 60 and 65535 for the number of seconds the router should wait between accelerated ping attempts, i.e. pings to the second destination address. Setting this to 0 disables the ping watchdog function
5. In the **Fail count** field, enter an integer between 1 and 65535 for the number of times an accelerated ping should fail before the router reboots. Setting this to 0 disables the ping watchdog function.

Disabling the Watchdog function

To disable the Watchdog reset function, set **Fail count** to 0.

Note: The traffic generated by the Watchdog feature is usually counted as chargeable data usage. Please keep this in mind when selecting how often to ping.

Configuring a periodic reboot

The router can be configured to automatically reboot after a period of time specified in minutes. While this is not necessary, it does ensure that in the case of remote installations, the router will reboot if some anomaly occurs.

1. In the **Force reboot every** field, enter the time in minutes between forced reboots. The default value is 0 which disables the Periodic reboot function. The minimum period between reboots is 5 minutes while the maximum value is 65535 minutes.
2. If you have configured a forced reboot time, you can use the **Randomize reboot time** drop down list to select a random reboot timer. Randomizing the reboot time is useful for preventing a large number of devices from rebooting simultaneously and flooding the network with connection attempts. When configured, the router waits for the configured **Force reboot every** time and then randomly selects a time that is less than or equal to the **Randomize reboot time** setting. After that randomly selected time has elapsed, the router reboots.
3. Click the **Save** button to save the settings.

Note: The randomize reboot time is not persistent across reboots; each time the router is due to reboot, it randomly selects a time less than or equal to the **Randomize reboot time**.

SNMP

SNMP configuration

The SNMP page is used to configure the SNMP features of the router.

Figure 86 - SNMP configuration

SNMP (Simple Network Management Protocol) is used to remotely monitor the router for conditions that may warrant administrative attention. It can be used to retrieve information from the router such as the signal strength, the system time and the interface status.

To configure SNMP:

1. Click the **SNMP** toggle key to switch it to the **ON** position.
2. Enter **Read-only community name** and **Read-write community name** which are used for client authentication.

Community names are used as a type of security to prevent access to reading and/or writing to the routers configuration. It is recommended that you change the Community names to something other than the default settings when using this feature.

3. Click the **Save** button to save any changes to the settings.

The **Download** button displays the Management information base (MIB) of the router. The MIB displays all the objects of the router that can have their values set or report their status. The MIB is formatted in the SNMP-related standard RFC1155.

SNMP traps

SNMP traps are messages from the router to the Network Management System sent as UDP packets. They are often used to notify the management system of any significant events such as whether the link is up or down.

Configuring SNMP traps

To configure SNMP traps:

1. In the **Trap destination** field, enter the IP address to which SNMP data is to be sent.
2. In the **Heartbeat interval** field, enter the number of seconds between SNMP heartbeats.
3. Use the **Trap persistence** field to specify the time in seconds that an SNMP trap persists.
4. Use the **Trap retransmission** time to specify the length of time in seconds between SNMP trap retransmissions.

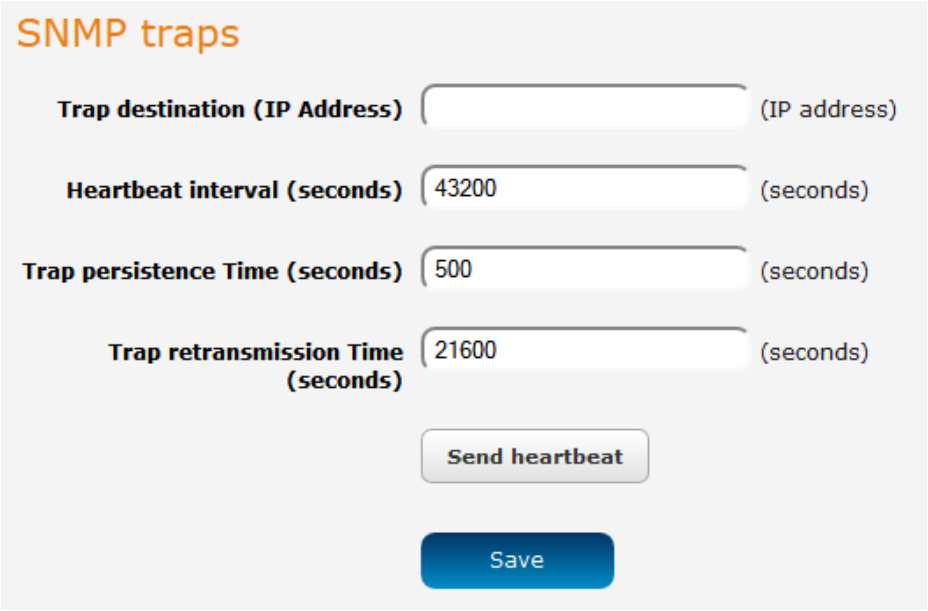


Figure 87 - SNMP traps

To send a manual SNMP Heartbeat, click the **Send heartbeat** button. When you have finished configuring the SNMP traps, click the **Save** button to save the settings.

TR-069

To access the TR-069 configuration page, click the **Services** menu item, then select the TR-069 menu item on the left.

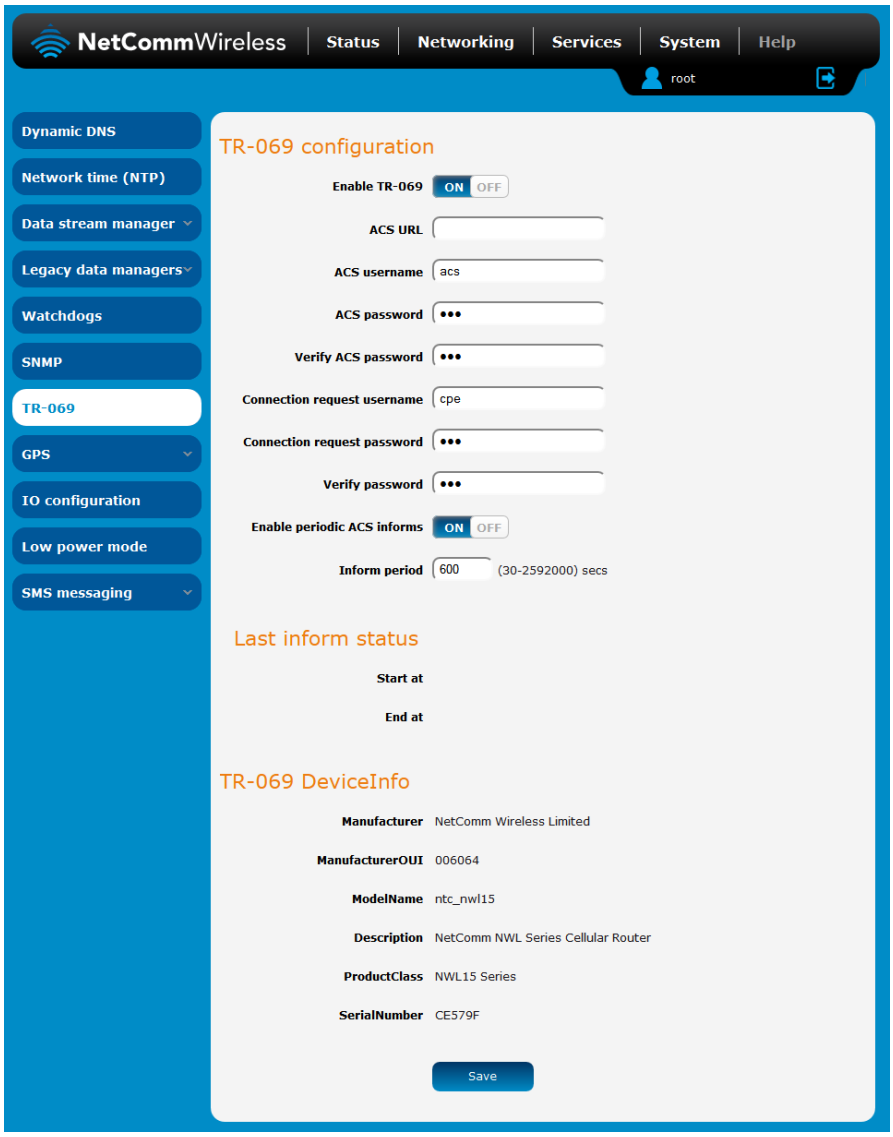


Figure 88 - TR-069 configuration

The TR-069 (Technical Report 069) protocol is a technical specification also known as CPE WAN Management Protocol (CWMP). It is a framework for remote management and auto-configuration of end-user devices such as customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It is particularly efficient in applying configuration updates across networks to multiple CPEs.

TR-069 uses a bi-directional SOAP/HTTP-based protocol based on the application layer protocol and provides several benefits for the maintenance of a field of CPEs:

- Simplifies the initial configuration of a device during installation
- Enables easy restoration of service after a factory reset or replacement of a faulty device
- Firmware and software version management
- Diagnostics and monitoring

Note:

- You must have your own compatible ACS infrastructure to use TR-069.
- When a factory reset of the router is performed via TR-069, the TR-069 settings are preserved.

TR-069 configuration

To configure TR-069:

1. Click the **Enable TR-069** toggle key to switch it to the **ON** position.
2. In the **ACS URL** field, enter the Auto Configuration Server's full domain name or IP address.
3. Use the **ACS username** field to specify the username for the Auto Configuration Server.
4. In the **ACS password** and **Verify ACS password** fields, enter the Auto Configuration Server password.
5. In the **Connection Request Username** field, enter the username to use for the connection requests.
6. In the **Connection Request Password** and Verify password fields, enter the connection request password.
7. The inform message acts as a beacon to inform the ACS of the existence of the router. Click the **Enable periodic ACS informs** toggle key to turn on the periodic ACS inform messages.
8. In the **Inform Period** field, enter the number of seconds between the inform messages.
9. Click the **Save** button to save the settings.

GPS

The built-in GPS module allows you to use location-based services, monitor field deployed hardware or find your current location. The GPS Status window provides up to date information about the current location and the current GPS signal conditions (position dilution of precision (PDOP), horizontal dilution of precision (HDOP) and vertical dilution of precision (VDOP)) of the router.

NMEA support

The router supports the National Marine Electronics Association NMEA-0183 compatible (V2.3) standard of sending GPS data. The standard includes "sentences" used to identify the type of data being sent and therefore defines the way the data is interpreted. The supported GPS related sentences are listed below:

- GPGGA – Global Positioning System Fix Data, Time, Position and fix related data for a GNSS receiver
- GPRMC – Recommended minimum data for GPS
- GPGSV – Detailed satellite data
- GPGSA – Overall satellite data
- GPVTG – Vector track and speed over the Ground

GPS configuration

To access the GPS configuration screen, select the **Services** item from the top menu bar then the **GPS** item on the left. Finally, select the **GPS configuration** menu item.

To use the GPS function, set the **GPS operation** toggle key to **ON** and click the **Save** button.

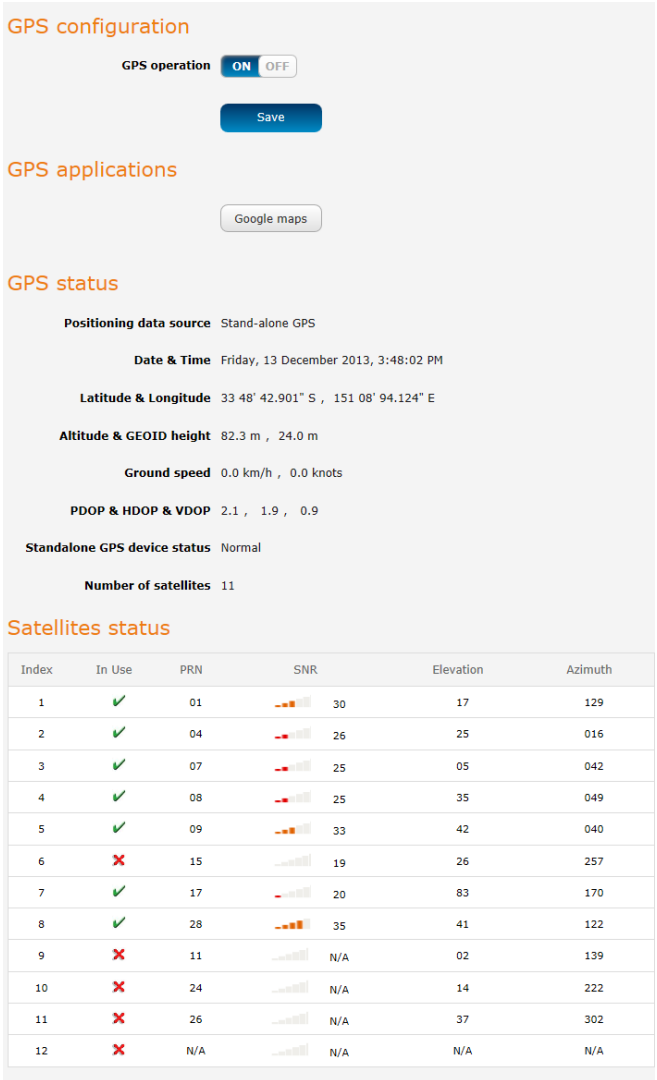

GPS configuration
GPS operation
ON
OFF
Save
GPS applications
Google maps
GPS status
Positioning data source Stand-alone GPS
Date & Time Friday, 13 December 2013, 3:48:02 PM
Latitude & Longitude 33 48' 42.901" S , 151 08' 94.124" E
Altitude & GEOID height 82.3 m , 24.0 m
Ground speed 0.0 km/h , 0.0 knots
PDOP & HDOP & VDOP 2.1 , 1.9 , 0.9
Standalone GPS device status Normal
Number of satellites 11
Satellites status
Index In Use PRN SNR Elevation Azimuth
1 ✔ 01 30 17 129
2 ✔ 04 26 25 016
3 ✔ 07 25 05 042
4 ✔ 08 25 35 049
5 ✔ 09 33 42 040
6 ✘ 15 19 26 257
7 ✔ 17 20 83 170
8 ✔ 28 35 41 122
9 ✘ 11 N/A 02 139
10 ✘ 24 N/A 14 222
11 ✘ 26 N/A 37 302
12 ✘ N/A N/A N/A N/A

Figure 89 – GPS configuration

The **Google maps** button provides a quick short cut to show your router's current position on a map

Mobile Station Based Assisted GPS configuration

To access the Mobile Station Based Assisted GPS configuration screen, select the **Services** item from the top menu bar then the **GPS** item on the left. Finally, select the **MSB (A-GPS)** menu item. This function is only available on models with built-in GPS capability.

Mobile Station Based Assisted GPS (MSB A-GPS) enables your router to download GNSS data which supply orbital data to GPS receiver, enabling it to lock to the satellites more rapidly.. The GNSS data is stored on the router to assist the GPS in locating the router.

To set up automatic updates of GNSS data, set the **A-GPS Enable** toggle key to the **ON** position and use the drop down lists to configure the automatic retry options. Each retry, the router checks for an updated GNSS data file and downloads the GNSS data if newer than the currently stored data.

Note: When new GNSS data is available and the router performs an update, up to 40MB of data may be downloaded. Please keep this in mind if your mobile broadband plan has usage restrictions.

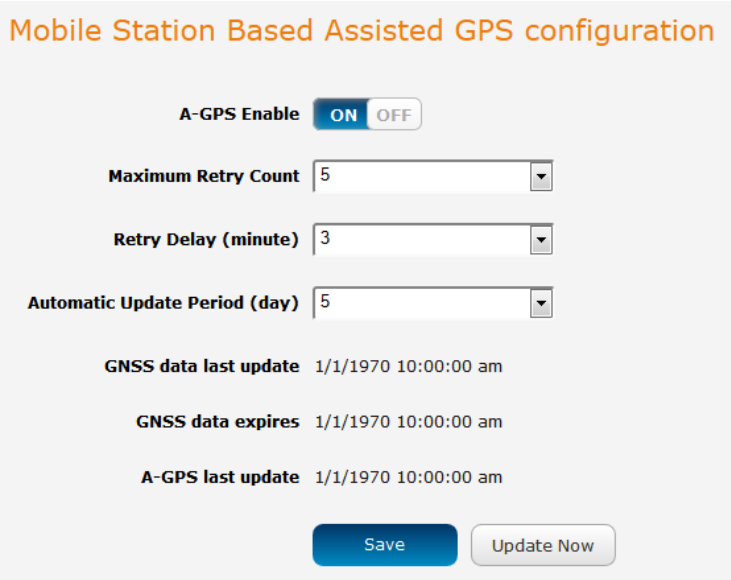


Figure 90 - Mobile Stations Based Assisted GPS configuration options

ITEM	DESCRIPTION
A-GPS Enable	Enables or disables the mobile station based assisted GPS function.
Maximum Retry Count	Sets the maximum number of times the router should attempt to triangulate its position.
Retry delay (minute)	Sets the number of minutes the router should wait between attempts to triangulate its position.
Automatic Update Period (day)	Sets the number of days that the router should automatically update the A-GPS data. The maximum update period is 7 days.

Table 17 - Mobile Station Based Assisted GPS configuration options

The **GNSS data last update** field represents the time that the GNSS data file was created while the **GNSS data expires** field indicates the time that this data is valid until. The **A-GPS last update** field specifies the last time the router attempted to retrieve an update to the GNSS data.

You may manually force the router to check for an update regardless of the next scheduled update time by clicking the **Update Now** button.

When you have finished configuring the settings, click the **Save** button to save the changes.

Odometer

To access the Odometer screen, select the **Services** item from the top menu bar then the **GPS** item on the left. Finally, select the **Odometer** menu item.

The GPS may be used to record the distance that the router has travelled. To do this, set the **Odometer** toggle key to the **ON** position as in the screenshot below. You can toggle the unit of measurement by clicking the **Display imperial / Display metric** button. The threshold setting adjusts the router's sensitivity to movement so that movement within the specified radius from the starting point does not register as distance travelled. When you have finished configuring the Odometer settings, click the **Save** button to ensure the settings are stored on the router.

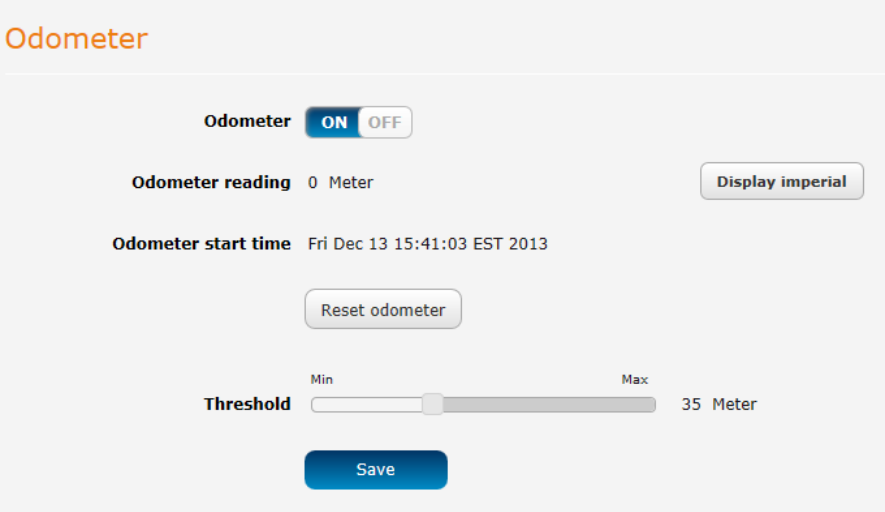


Figure 91 – Odometer options

ITEM	DESCRIPTION
Odometer reading	The number of metres/kilometres that the device has travelled since the time listed in the Odometer start time field.
Display imperial / Display metric	Toggles the Odometer reading between metric and imperial measurements.
Odometer start time	The time that recording of distance travelled began.
Reset odometer	Resets the odometer reading to 0 and the Odometer start time to the current time.
Odometer	Toggles the Odometer function on and off.
Threshold	Specifies the minimum distance that the router must travel from its current position before the Odometer reading increases.

Table 18 - Odometer configuration options

IO configuration

The NWL-15 router is equipped with a 6-way terminal block connector providing 3 identical multipurpose inputs and outputs as well as a dedicated ignition input. These inputs and outputs may be independently configured for various functions, including:

- NAMUR (EN 60947-5-6 / IEC 60947-5-6) compatible proximity sensor input
- Proximity sensor input for use with contact closure (open/closed) type of sensors (PIR sensors, door/window sensors for security applications) with the input tamper detection possible (four states detected: open, closed, short and break) by the use of external resistors
- Analogue 0V to 30V input
- Digital input (the I/O voltage measured by the iMX283 LRADC and the software making decision about the input state) with the threshold levels configurable in software
- Open collector output.

Use the pull up voltage options to select the desired output voltage of the I/O pins. The pull up voltage you select will be the same for each pin when pull up is enabled for that pin. Each pin is capable of outputting either 3.3V or 8.2V.

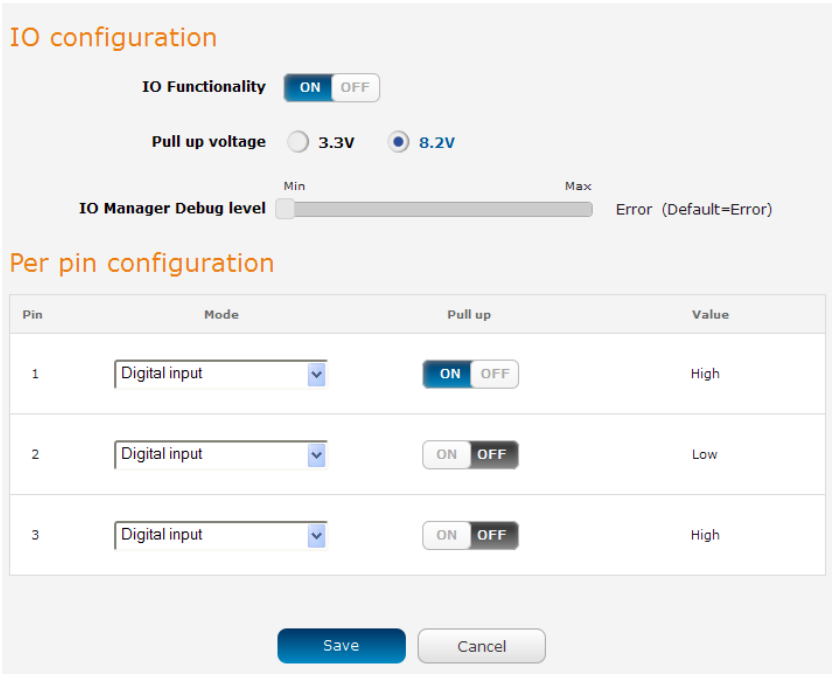


Figure 92 – IO configuration options

ITEM	DESCRIPTION
IO configuration	
IO Functionality	Enables the configuration of the input and output pins on the Six-way terminal block.
Pull up voltage	Specifies the output voltage of the I/O pins.
IO Manager Debug level	Use the slide bar to adjust the level of detail you would like to see in the log for IO messages. A higher debug level displays more detailed messages in the log file.
Per pin configuration	
Pin	The I/O pin number corresponding to the pin on the terminal block.
Mode	The mode of operation for the corresponding pin. Available options are Digital input, Digital output, Analogue input, Namur input, Contact closure input.
Pull up	Use the pull up toggle keys to turn the pull up on or off for the corresponding pin. When turned on, the pull up voltage output is the value specified in the "Pull up voltage" option.
Value	The value column displays whether the voltage detected on the line is low or high or allows you to configure the output value in the case that the pin is set to digital output This can be useful for applications where monitoring of the transition between low and high is used to trigger an action.

Table 19 - IO configuration options

The table below describes the different modes available on the physical I/O pins of the router.

MODE	DESCRIPTION
Digital input	The corresponding pin accepts digital input. Pull up may be on or off and both 3.3V and 8.2V are available as pull up voltages. The value column displays whether the signal received on the pin is High or Low.
Digital output	The corresponding pin outputs a digital signal. Pull up may be on or off and both 3.3V and 8.2V are available as pull up voltages. The value column contains a toggle key allowing you to set whether the output signal is High or Low.
Analogue input	The corresponding pin accepts an analogue signal. Pull up may be on or off and both 3.3V and 8.2V are available as pull up voltages. The value column displays the current voltage detected on the pin.
Namur input	NAMUR is a sensor standard using low-level current signals. It can supply two different signal levels depending on the state of the switch and is commonly used in hazardous or explosive locations where compact sensors are required. When a pin is set to NAMUR mode, Pull up is turned on and the global Pull up voltage is set to 8.2V. These settings may not be changed for as long as a pin is set to NAMUR mode as they are required settings according to the NAMUR IEC 60947-5-6 standard. The value column displays whether the signal received on the pin is High or Low.
Contact closure input	A common type of digital input where a sensor or switch opens or closes a set of contacts as a result of a process change. An electrical signal is then used to determine whether the circuit is open or closed. When a pin is set to Contact closure input, Pull up is enabled for that pin and may not be turned off as long as the pin remains configured as a Contact closure input. Global pull up voltage may be either 3.3V or 8.2V.

Table 20 - IO configuration options

Note: Please refer to the SDK Developer Guide for hardware information about the Input/Output pins, wiring examples and configuration of the pins via the command line interface. There are also wiring examples in Appendix I of this User Guide. Contact NetComm Wireless Technical Support for access to the Software Development Kit.

Low power mode

The NWL-15 router can be configured to enter or return from a low power 'sleep' mode. You can configure this to occur automatically after a timer has expired, by the status of the ignition pin, a combination of timer and ignition pin status or by manually triggering sleep mode.

During the sleep state, the NWL-15 router is effectively powered off. That is, it has no ability to communicate wirelessly or process any information. When in sleep mode, it draws approximately 5mA current at 12V. When sleep state is triggered, the NWL-15 router takes approximately 30 seconds to enter low power mode. When the wake up sequence is initiated, the router takes approximately 2 minutes to return from the sleep state. This is because returning from sleep state involves a full boot up sequence.

Ignition pin

The third pin on the 6-way terminal connector is a dedicated input called "Ignition". This input is intended for connection to an ignition switch in vehicular applications or where an input to switch the device to a sleep/wake mode is required.

The Ignition input threshold voltage is around 3V. The input responds to a high input state (above 3V). A signal below this level is considered as a low state. If the software is configured to activate in the low state, for example 0V, it must still have the high state above 3V to turn it off.

Note: There is a period of about 10 seconds after sleep state has been triggered where the ignition line cannot be monitored. Please take this into account when designing your ignition power on system.

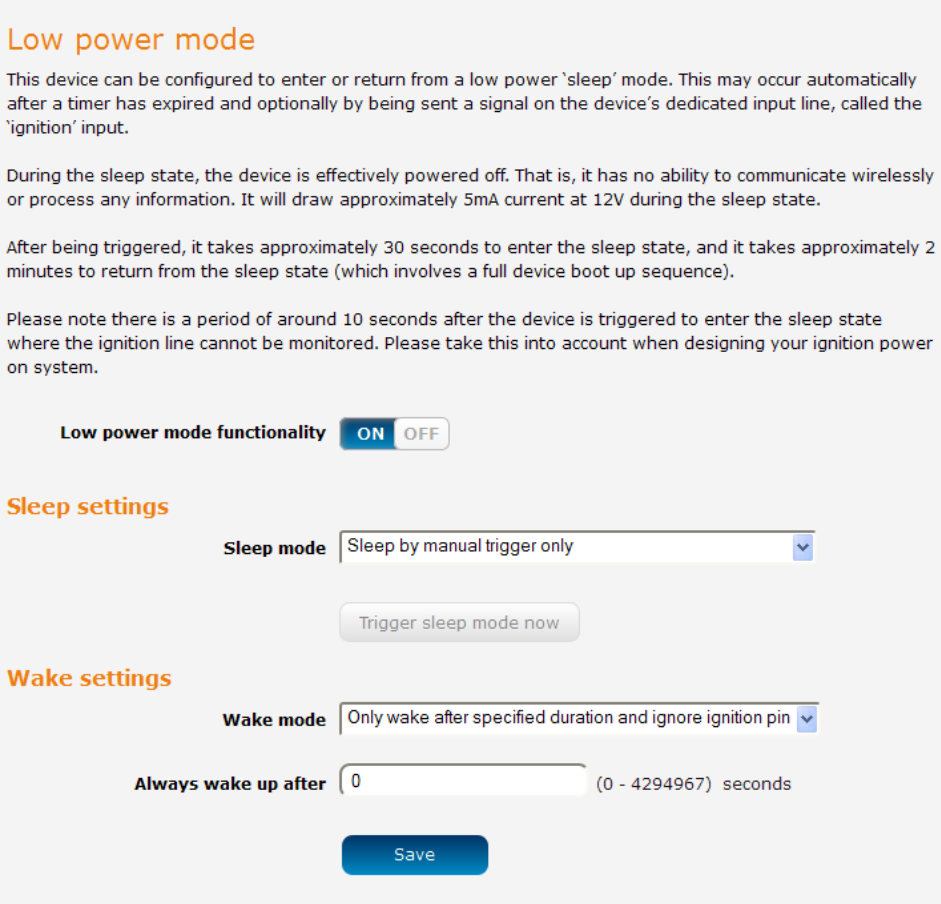

Low power mode
This device can be configured to enter or return from a low power 'sleep' mode. This may occur automatically after a timer has expired and optionally by being sent a signal on the device's dedicated input line, called the 'ignition' input.
During the sleep state, the device is effectively powered off. That is, it has no ability to communicate wirelessly or process any information. It will draw approximately 5mA current at 12V during the sleep state.
After being triggered, it takes approximately 30 seconds to enter the sleep state, and it takes approximately 2 minutes to return from the sleep state (which involves a full device boot up sequence).
Please note there is a period of around 10 seconds after the device is triggered to enter the sleep state where the ignition line cannot be monitored. Please take this into account when designing your ignition power on system.
Low power mode functionality
ON
OFF
Sleep settings
Sleep mode
Sleep by manual trigger only
Trigger sleep mode now
Wake settings
Wake mode
Only wake after specified duration and ignore ignition pin
Always wake up after
0
(0 - 4294967) seconds
Save

Figure 93 - Low power mode settings

To begin using Low power mode, set the **Low power mode functionality** toggle key to the **ON** position. Extra settings are displayed. These settings, including the enabling or disabling of Low power mode functionality, only take effect when you click the **Save** button.

Sleep settings

Use the **Sleep mode** drop down list to select a condition under which the router should enter the sleep state.

Sleep by manual trigger only

When this mode is selected, the router will only enter the sleep state when the **Trigger sleep mode now** button is pressed. The **Trigger sleep mode now** button is not available unless Low power functionality has been selected and the setting saved.

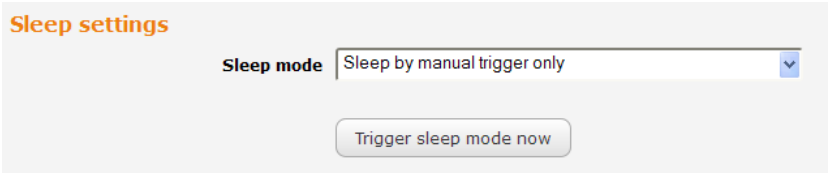


Figure 94 - Sleep by manual trigger only

Sleep after specified duration and ignore ignition pin

When this mode is selected, the router goes to sleep after the specified time period regardless of the state of the ignition pin.

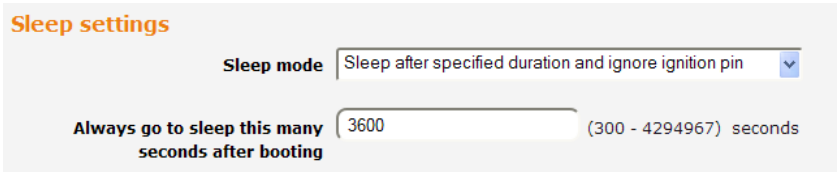

Sleep settings
Sleep mode
Sleep after specified duration and ignore ignition pin
Always go to sleep this many seconds after booting
3600
(300 - 4294967) seconds

Figure 95 - Sleep after specified duration and ignore ignition pin

Enter the time in seconds to wait before entering sleep state in the **Always go to sleep this many seconds after booting** field. A setting of 0 means that the router will never enter sleep state.

Sleep triggered by ignition pin status

This mode sets the router to enter sleep state when the signal on the ignition pin reaches the specified value.

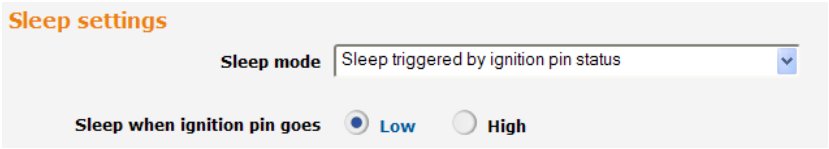


Figure 96 - Sleep triggered by ignition pin status

Use the **Sleep when ignition pin goes** setting to select **Low** or **High**. By default, this is set to **Low.**

Sleep after specified duration or triggered by ignition pin

This option sets the router to go to the sleep state on one of two conditions, depending on which condition is reached first. These conditions are based on the state of the ignition pin and a timer. For example, based on the configuration in the screenshot below, the router will go to sleep state when the ignition pin goes low or after 3600 seconds (1 hour), depending on which condition occurs first.

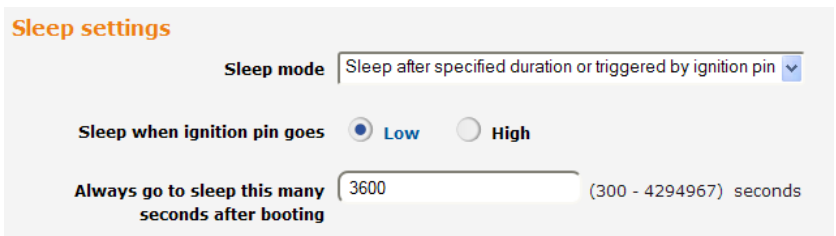


Figure 97 - Sleep after specified duration or triggered by ignition pin

Wake settings

Use the **Wake mode** drop down list to select a condition under which the router should return from the sleep state.

Only wake after specified duration and ignore ignition pin

When this mode is selected, the router wakes up after the specified time period regardless of the state of the ignition pin.

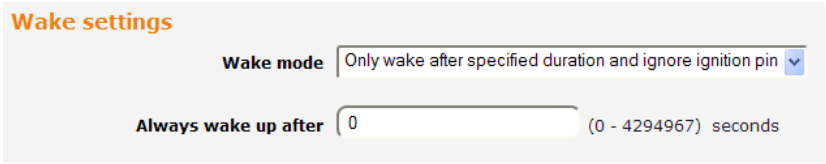


Figure 98 - Only wake after specified duration and ignore ignition pin

Enter the time in seconds to wait before returning from sleep state in the **Always wake up after** field. A setting of 0 means that the router will automatically wake from sleep state immediately.

Wake triggered by ignition pin status

This mode sets the router to wake up when the signal on the ignition pin reaches the specified value.

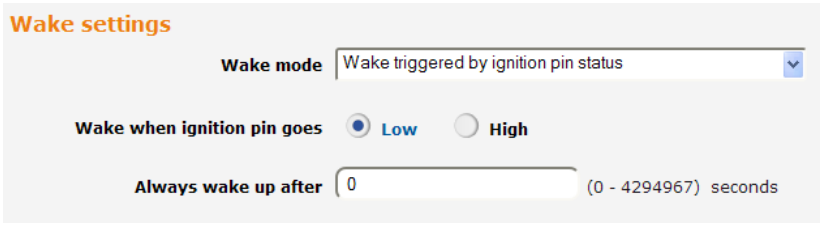


Figure 99 - Wake when triggered by ignition pin status

Use the **Sleep when ignition pin goes** setting to select **Low** or **High**. By default, this is set to **Low.**

Advanced wake settings

The advanced wake settings screen gives you finer control over the events causing the router to wake up. In advanced wake mode, you can configure the router to monitor for up to 2 changes in the status of the ignition pin along with how long those status changes should last for to trigger a single wake up event. When selected, Event 1 and Event 2 must happen consecutively in that order to satisfy each condition.

Note: If you do not wish to specify 2 events you should select to skip Event 1, in which case the router will only monitor Event 2 to trigger a wake up.

There is also a provision to reboot the router after a specified period of time, regardless of whether the conditions of Events 1 and/or 2 are met. This can be viewed as a fall back option in the case that those Events are missed.

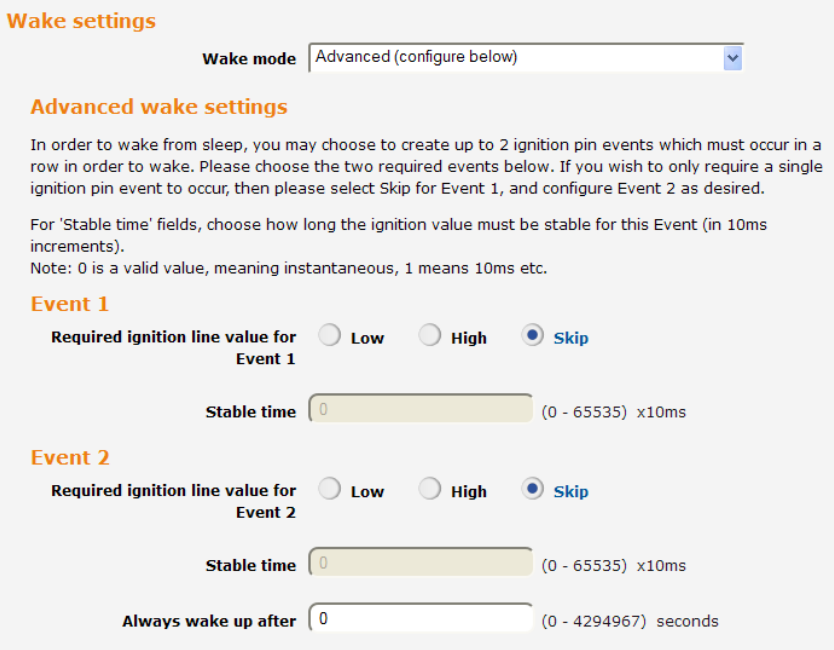

Wake settings
Wake mode
Advanced (configure below)
Advanced wake settings
In order to wake from sleep, you may choose to create up to 2 ignition pin events which must occur in a row in order to wake. Please choose the two required events below. If you wish to only require a single ignition pin event to occur, then please select Skip for Event 1, and configure Event 2 as desired.
For 'Stable time' fields, choose how long the ignition value must be stable for this Event (in 10ms increments).
Note: 0 is a valid value, meaning instantaneous, 1 means 10ms etc.
Event 1
Required ignition line value for Event 1
Low
High
Skip
Stable time
0
(0 - 65535) x10ms
Event 2
Required ignition line value for Event 2
Low
High
Skip
Stable time
0
(0 - 65535) x10ms
Always wake up after
0
(0 - 4294967) seconds

Figure 100 - Advanced wake up configuration

To configure advanced wake settings:

1. Set **Wake mode** to Advanced (configure below).
2. Under **Event 1**, select whether you want the ignition pin value to be Low or High. If you want to skip this event, select the Skip option.
3. In the Event 1 **Stable time** field, enter the length of time expressed in milliseconds that the value of the ignition line should remain low or high. For example, to specify 10 seconds, enter a value of 1000.
4. Under **Event 2**, select whether you want the ignition pin value to be Low or High. If you want to skip this event, select the Skip option.
5. In the Event 2 **Stable time** field, enter the length of time expressed in milliseconds that the value of the ignition line should remain low or high.
6. In the **Always wake up after** field, enter the time in seconds after which the router should wake up, regardless of whether Event 1 or 2 has occurred.

When in low power mode and Advanced wake mode is configured, the router waits for Event 1 to occur, then it monitors for Event 2. If Event 2 occurs before Event 1, it will not trigger the condition for either event to have occurred. If Event 1 occurs and then Events 2 occurs, the router wakes up. Alternatively, if neither or only one of the events occurs, the router waits for the time specified in the **Always wake up after** field and then wakes up when that time has been reached.

SMS

The NWL-15 router offers an advanced SMS feature set, including sending messages, receiving messages, redirecting incoming messages to another destination, as well as supporting remote commands and diagnostics messages.

Some of the functions supported include:

- Ability to send a text message via a CDMA network and store it in permanent storage.
- Ability to receive a text message via a CDMA network and store it in permanent storage.
- Ability to forward incoming text messages via a CDMA network to another remote destination which may be a TCP/UDP server or other mobile devices.
- Ability to receive run-time variables from the device (e.g. uptime) on request via SMS
- Ability to change live configuration on the device (e.g. network username) via SMS.
- Ability to execute supported commands (e.g. reboot) via SMS
- Ability to trigger the NWL-15 router to download and install a firmware upgrade
- Ability to trigger the NWL-15 router to download and apply a configuration file

To access the SMS messaging functions of the NWL-15 router, click on the **Services** menu item from the top menu bar, and then select one of the options under the **SMS messaging** section on the left hand menu.

Setup

The Setup page provides the options to enable or disable the SMS messaging functionality and SMS forwarding functionalities of the router. SMS messaging is enabled by default.

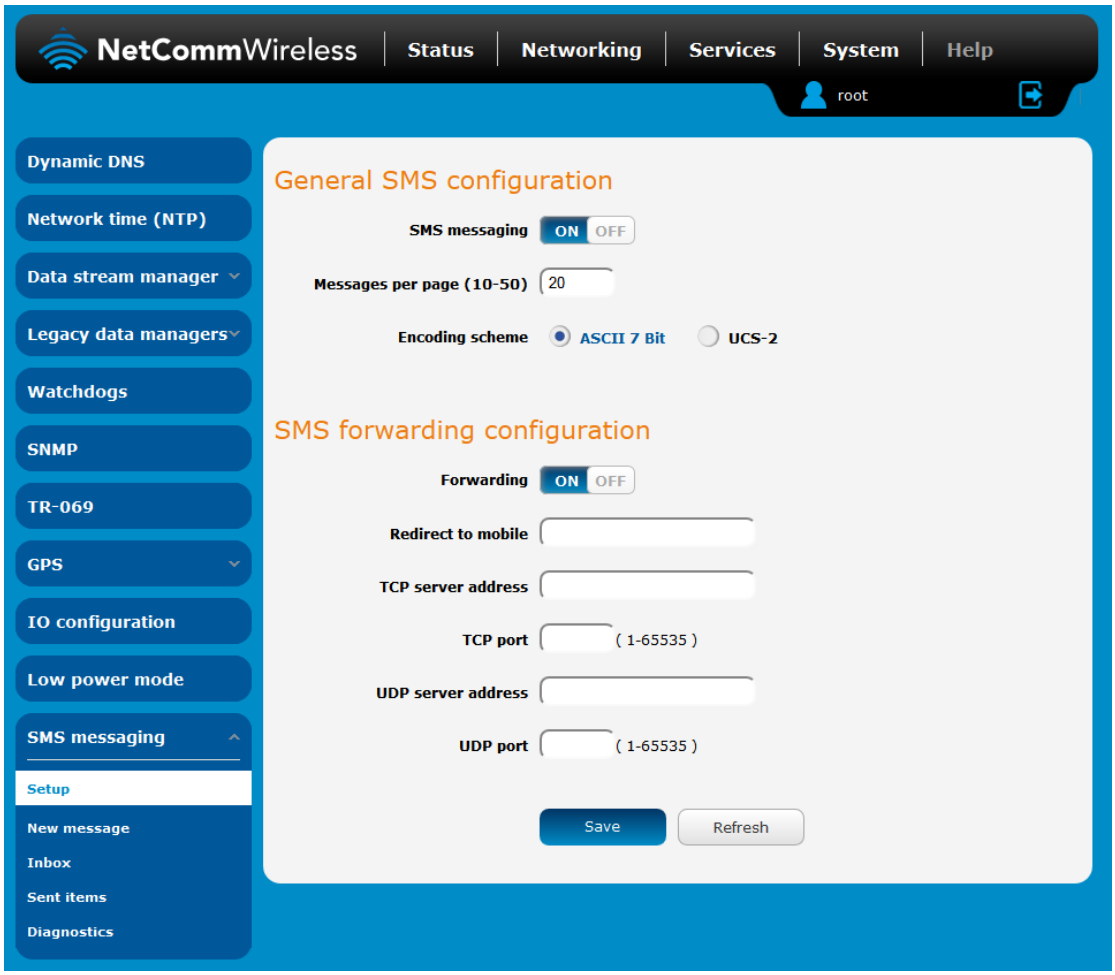


Figure 101 - General SMS Configuration

OPTION	DEFINITION
General SMS Configuration	
SMS	Toggles the SMS functionality of the router on and off.
Messages Per Page (10-50)	The number of SMS messages to display per page. Must be a value between 10 and 50.
Encoding Scheme	The encoding method used for outbound SMS messages. GSM 7-bit mode permits up to 160 characters per message but drops to 50 characters if the message includes special characters. UCS-2 mode allows the sending of Unicode characters and permits a message to be up to 50 characters in length.
SMS Forwarding Setup	
Forwarding	Toggles the SMS forwarding function of the router on and off.
Redirect to Mobile	Enter a mobile number as the destination for forwarded SMS messages.
TCP server IP address	Enter an IP address or domain name as the destination for forwarded SMS messages using TCP.
TCP Port	The TCP port on which to connect to the remote destination.
UDP server IP address	Enter an IP address or domain name as the destination for forwarded SMS messages using UDP.
UDP Port	The UDP port on which to connect to the remote destination.

Table 21 - SMS Setup Settings

SMS forwarding setup

Incoming text messages can be redirected to another mobile device and/or a TCP/UDP message server.

Redirect to mobile

You can forward incoming text messages to a different destination number. This destination number can be another mobile phone or a 3G router phone number.

For Example:

If someone sends a text message and **Redirect to mobile** is set to "+01161412345678", the text message is stored on the router and forwarded to "+01161412345678" at the same time.

To disable redirection to a mobile, clear the **Redirect to mobile** field and click the **Save** button.

Redirect to TCP / UDP address

You can also forward incoming text messages to a TCP/UDP based destination. The TCP or UDP server can be any kind of public or private server if the server accepts incoming text-based messages.

The TCP/UDP address can be an IP address or domain name. The port number range is from 1 to 65535. Please refer to your TCP/UDP based SMS server configuration for which port to use.

For Example:

If someone sends a text message and **TCP address** is set to "192.168.20.3" and **TCP port** is set to "2002", this text message is stored in the router and forwarded to "192.168.20.3" on port "2002" at the same time.

To disable redirection to a TCP or UDP address, clear the **TCP address** and **UDP address** fields and click the **Save** button.

New message

The New message page can be used to send SMS text messages to a single or multiple recipients.

A new SMS message can be sent to a maximum of 9 recipients at the same time. After sending the message, the result is displayed next to the destination number as "Success" or "Failure" if the message failed to send. By default, only one destination number field is displayed. Additional destination numbers may be added one at a time after entering a valid number for the current destination number field. To add a destination number, click the + button and to remove the last destination in the list, click the − button.

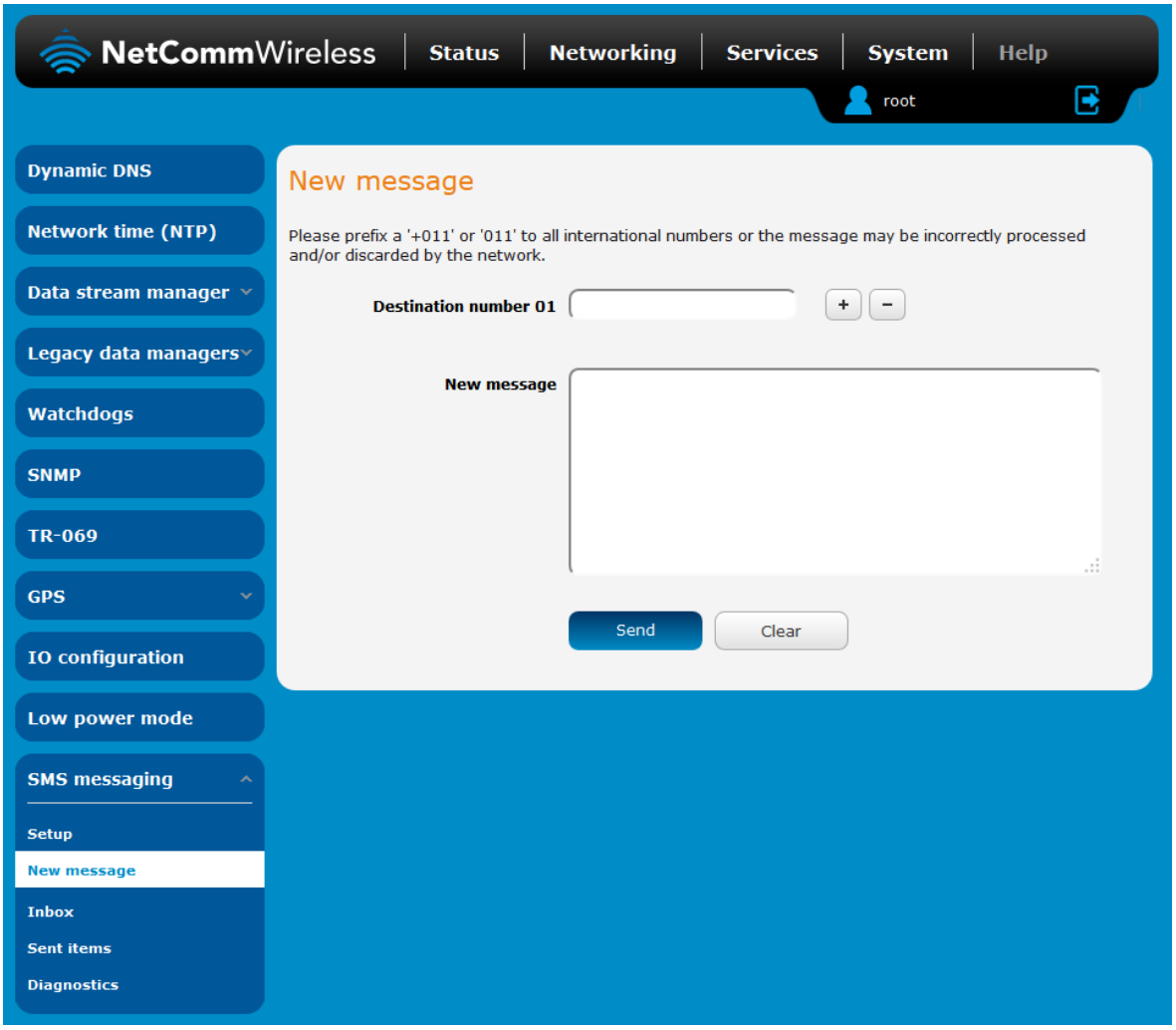


Figure 102 - SMS - New Message

When sending SMS messages internationally, destination numbers may begin with the "+" symbol followed by the international direct dial prefix and then the country calling code or you may choose to omit the "+" symbol.

For example:

To send a message to the mobile destination number 0412345678 in Australia (country calling code 61) from the United States, enter "+01161412345678" or "01161412345678".

After entering the required recipient numbers, type your SMS message in the **New message** field. As you type your message, a counter shows how many characters you have entered. For ASCII 7-Bit encoding, the maximum number of characters is 160 per message while UCS2 encoding allows 50 characters per message. If your message exceeds these numbers, it will be split into multiple messages as required. When you have finished typing your message and you are ready to send it, click the **Send** button.

Inbox / Sent items

The Inbox displays all received messages that are stored on the router while the Outbox displays all sent messages.

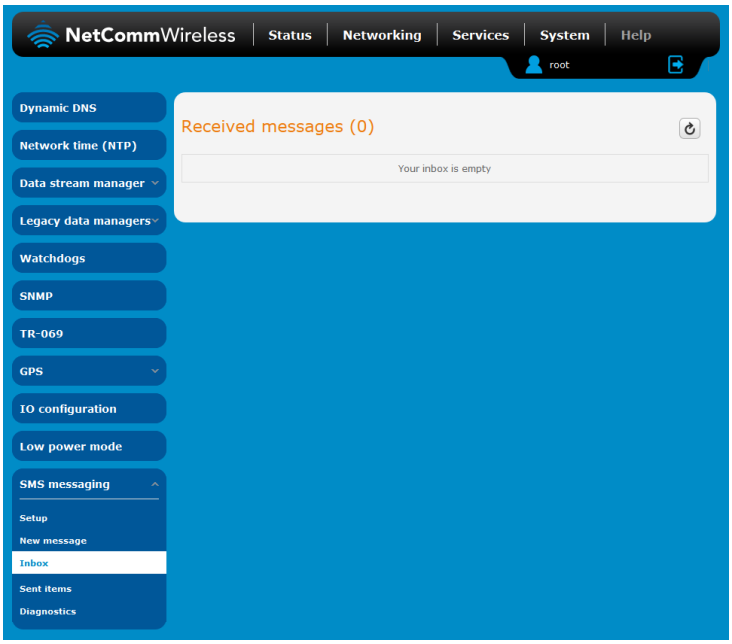


Figure 103 - SMS Inbox

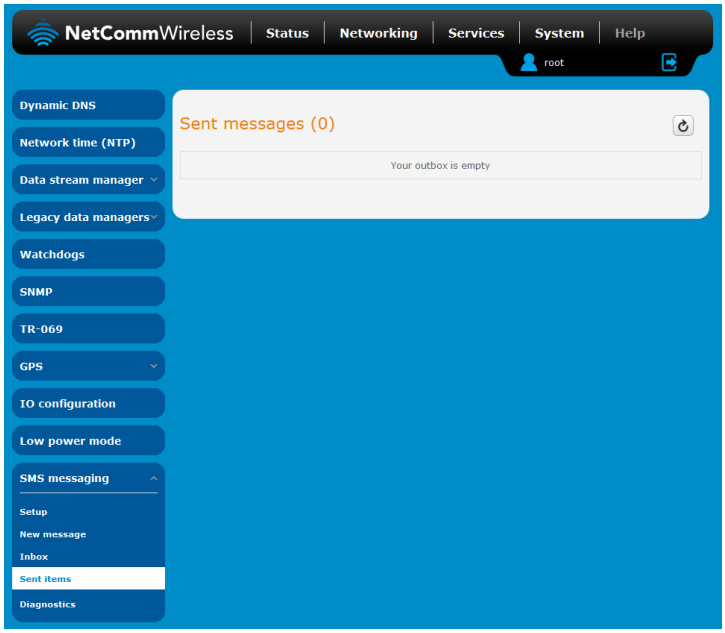


Figure 104 - SMS Outbox

ICON	DESCRIPTION
	Forward button. Click this button to open a new message window where you can forward the corresponding message to another recipient.
	Reply button. Click this button to open a new message window where you can reply to the sender.
	Add to White list. Click this button to add the sender's mobile number to the white list on the router.
	Delete button. Click this button to delete the corresponding message.
	Refresh button. Click this button to refresh the inbox or outbox to see new messages.

Table 22 - Inbox/Outbox icons

Diagnostics

The Diagnostics page is used to configure the SMS diagnostics and command execution configuration. This enables you to change the configuration, perform functions remotely and check on the status of the router via SMS commands.

To access the Diagnostics page, click on the **Services** menu item then select the **SMS messaging** menu on the left and finally select **Diagnostics** beneath it.

NetCommWireless
Status
Networking
Services
System
Help
root
Dynamic DNS
Network time (NTP)
Data stream manager
Legacy data managers
Watchdogs
SNMP
TR-069
GPS
IO configuration
Low power mode
SMS messaging
Setup
New message
Inbox
Sent items
Diagnostics
SMS diagnostics and command execution configuration
Enable remote diagnostics and command execution
Only accept authenticated SMS messages
Send Set command acknowledgement replies
Access advanced RDB variables
Allow execution of advanced commands
Send acknowledgement replies to
a fixed number
the sender's number
Send command error replies
Send error replies to
Send a maximum number of
100
replies per
day
0 / 100 messages sent
Limit the number of diagnostic text messages that can be sent in a designated time period. Currently, the 'messages sent' count automatically resets at the start of the designated time period. For example, it will reset to zero at 01:00, 02:00, 03:00 etc for 'hour', 00:00 for 'day', 00:00 on Monday for 'week' and the first day of the month for 'month'.
White list for diagnostic or execution SMS
All incoming diagnostic or execution text messages are checked against this white list. If the message sender and password don't match any destination numbers and passwords in this white list, the message is ignored and an error message reply is sent to the sender or to a predefined destination. You can add up to 20 destination numbers via the SMS inbox/outbox pages by clicking on 'Add white list'. Alternatively, click on 'Add' below to add a number now.
+ Add
The white list is empty
Save
Refresh

Figure 105 - SMS diagnostics and command execution configuration

SMS diagnostics and command execution configuration

The options on this page are described below.

Enable remote diagnostics and command execution

Enables or disables the remote diagnostics feature. If this setting is enabled all incoming text messages are parsed and tested for remote diagnostics commands.

If remote diagnostics commands are found, the router executes those commands. This feature is enabled by default. All remote diagnostic commands that are received are stored in the Inbox.

Note: It is possible to adjust settings and prevent your router from functioning correctly using remote diagnostics. If this occurs, you will need to perform a factory reset in order to restore normal operation.

We highly recommended that you use the white list and a password when utilising this feature to prevent unauthorised access. See the White list description for more information.

Only accept authenticated SMS messages

Enables or disables checking the sender's phone number against the allowed sender white list for incoming diagnostics and command execution SMS messages.

If authentication is enabled, the router will check if the sender's number exists in the white list. If it exists, the router then checks the password (if configured) in the incoming message against the password in the white list for the corresponding sending number. If they match, the diagnostic or command is executed.

If the number does not exist in the white list or the password does not match, the router does not execute the incoming diagnostic or command in the SMS message.

This is enabled by default and it is strongly advised that you leave this feature enabled to maintain security.

Send Set command acknowledgement replies

The NWL-15 router will automatically reply to certain types of commands received, such as *get* commands, or *execute* commands. However acknowledgement replies from the NWL-15 router are optional with *set* commands and the *Wakeup* command. This option Enables or disables sending an acknowledgment message after execution of a *set* command or SMS Wakeup command. If disabled, the router does not send any acknowledgement after execution of a *set* command or SMS Wakeup command. All acknowledgment replies are stored in the Outbox after they have been sent. This can be useful to determine if a command was received and executed by the router. This option is disabled by default.

Access advanced RDB variables

By default, this option is turned off and only allows access to the basic RDB variables listed later in this guide. If this option is enabled, you are able to access the full list of RDB variables via SMS.

Allow execution of advanced commands

By default, this option is turned off and only allows execution of the basic commands listed later in this guide. If this option is enabled, you are able to execute advanced commands such as those which are common to the Linux command line. For example: "execute ls /usr/bin/sms*" to list the contents of the /etc folder on the router.

Send acknowledgement replies to

This option allows you to specify where to send acknowledgment messages after the execution of a *set, get,* or *exec* command.

If **a fixed number** is selected, the acknowledgement message will be sent to the number defined in the **Fixed number to send replies to** field. If **the sender's number** is selected, the acknowledgement message will be sent to the number that the SMS diagnostic or command message originated from. The default setting is to use **the sender's number**.

Fixed number to send replies to

This field defines the destination number to which error messages are sent after the execution of a *get*, *set,* or *exec* command. This field is only displayed when **Send Error SMS to** is set to **Fixed Number**.

Send command error replies

Enables or disables the sending of an error message resulting from the execution of a *get*, *set*, or *exec* command. All error replies are stored in the Outbox after they have been sent.

Send error replies to

When **Send Error SMS for Get/Set/Exec Command** is set to **ON**, this option is used to specify where the error SMS is sent. Use the radio buttons to select either **Fixed Number** or **SMS Sender Number**. When set to **SMS Sender Number** the router will reply to the originating number of the SMS diagnostic or command. When set to **Fixed Number** the router will send the error messages to the number specified in the following field.

Send a maximum number of

You can set the maximum number of acknowledgement and error messages sent when an SMS diagnostic or command is executed. The maximum limit can be set per hour, day, week or month. The router will send a maximum of 100 replies by default.

The number of messages sent is shown below the options. The total transmitted message count resets after a reboot or at the beginning of the time frame specified.

White list for diagnostic or execution SMS

The white list is a list of mobile numbers that you can create which are considered “friendly” to the router. If **Only accept authenticated SMS messages** is enabled in the diagnostics section, the router will compare the mobile number of all incoming diagnostic and command messages against this white list to determine whether the diagnostic or command should be executed. You may optionally configure a password for each number to give an additional level of security. When a password is specified for a number, the SMS diagnostic or command message is parsed for the password and will only be executed if the number and password match.

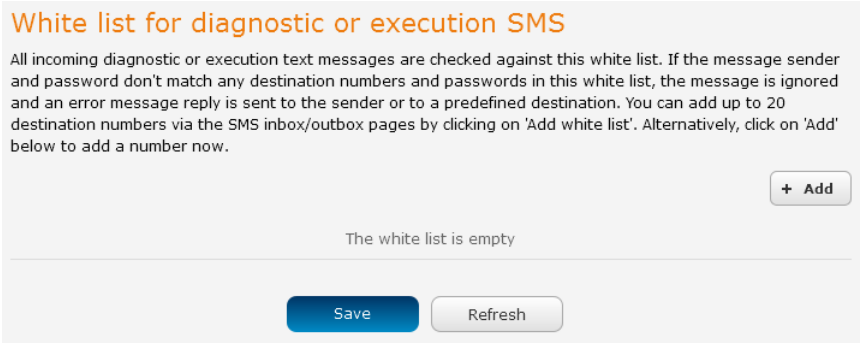

White list for diagnostic or execution SMS
All incoming diagnostic or execution text messages are checked against this white list. If the message sender and password don't match any destination numbers and passwords in this white list, the message is ignored and an error message reply is sent to the sender or to a predefined destination. You can add up to 20 destination numbers via the SMS inbox/outbox pages by clicking on 'Add white list'. Alternatively, click on 'Add' below to add a number now.
+ Add
The white list is empty
Save
Refresh

Figure 106 - White list for diagnostic or execution SMS

A maximum of 20 numbers can be stored on the router in the white list. To add a number to the white list, click the “**+Add**” button.

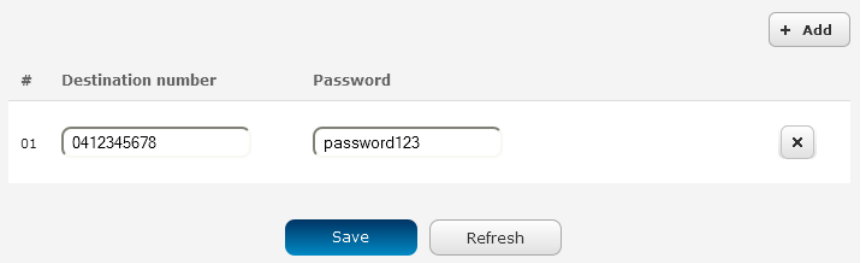


Figure 107 – Adding a number to the SMS white list

The White List numbers and passwords can be cleared by pressing the × button to the right of each entry. To add a number to the white list, enter it in the **Destination number** field and optionally define a password in the **Password** field. When you have finished adding numbers click the **Save** button to save the entries.

Sending an SMS diagnostic command

Follow the steps below to configure the router to optionally accept SMS diagnostic commands only from authenticated senders and learn how to send SMS diagnostic commands to the router.

1. Navigate to the Services > SMS messaging > Diagnostics page
2. Confirm that the **Enable remote diagnostics and command execution** toggle key is set to the **ON** position. If it is set to **OFF** click the toggle key to switch it to the **ON** position.
3. If you wish to have the router only accept commands from authenticated senders, ensure that **Only accept authenticated SMS messages** is set to the **ON** position. In the **White list for diagnostic or execution SMS messages** section, click the **+Add** button and enter the sender's number in international format into the **Destination number** field that appears. If you wish to also configure a password, enter the password in the **Password** field corresponding to the destination number.
4. If you would prefer to accept SMS diagnostic commands from any sender, set the **Only accept authenticated SMS messages** toggle key to the **OFF** position.

Note: An alternative method of adding a number to the white list is to send an SMS message to the router, navigate to **Services > SMS messaging > Inbox** and then click the button next to the message which corresponds to the sender's number.

5. Click the **Save** button.

Types of SMS diagnostic commands

There are three types of commands that can be sent; **execute**, **get** and **set.** The basic syntax is as follows:

- execute COMMAND
- get VARIABLE
- set VARIABLE=VALUE

If authentication is enabled, each command must be preceded by the password:

- PASSWORD execute COMMAND
- PASSWORD get VARIABLE
- PASSWORD set VARIABLE=VALUE

The following are some examples of SMS diagnostic commands:

- password6657 execute reboot
- get rssi
- set apn1=testAPNvalue

SMS acknowledgment replies

The router automatically replies to **get** commands with a value and **execute** commands with either a success or error response. **Set** commands will only be responded to if the **Send Set command acknowledgement replies** toggle key is set to **ON**. If the **Send command error replies** toggle key is set to **ON**, the router will send a reply if the command is correct but a variable or value is incorrect, for example, due to misspelling.

SMS command format

Generic Format for reading variables:

get VARIABLE

PASSWORD get VARIABLE

Generic Format for writing to variables:

set VARIABLE=VALUE

PASSWORD set VARIABLE=VALUE

Generic Format for executing a command:

Execute COMMAND

PASSWORD execute COMMAND

Replies

Upon receipt of a successfully formatted, authenticated (if required) command, the gateway will reply to the SMS in the following format:

TYPE	SMS CONTENTS	NOTES
get command	"VARIABLE=VALUE"	
set command	"Successfully set VARIABLE to VALUE"	Only sent if the acknowledgment message function is enabled
execute command	"Successfully executed command COMMAND"	

Table 23 - SMS Diagnostic Command Syntax

Where "VARIABLE" is the name of the value to be read

Where "VARIABLE (x)" is the name of another value to be read

Where "VALUE" is the content to be written to the "VARIABLE"

Where "COMMAND" is a supported command to be executed by the device (e.g. reboot)

Where "PASSWORD" is the password (if configured) for the corresponding sender number specified in the White List

Multiple commands can be sent in the same message, if separated by a semicolon.

For Example:

get VARIABLE1; get VARIABLE2; get VARIABLE3

PASSWORD get VARIABLE1; get VARIABLE2

set VARIABLE=VALUE1 ; set VARIABLE2=VALUE2

PASSWORD set VARIABLE1=VALUE1; set VARIABLE2=VALUE2; set VARIABLE3=VALUE3

If required, values can also be bound by an apostrophe, double apostrophe or back tick.

For Example:

"set VARIABLE='VALUE'"

"set VARIABLE="VALUE""

"set VARIABLE=`VALUE`"

"get VARIABLE"

A password (if required), only needs to be specified once per SMS, but can be prefixed to each command if desired.

“PASSWORD get Variable1”; “get VARIABLE2”

“PASSWORD set VARIABLE1=VALUE1”; “set VARIABLE2=VALUE2”

If the command sent includes the “reboot” command and has already passed the white list password check, the device keeps this password and executes the remaining command line after the reboot with this same password.

For Example:

“PASSWORD execute reboot; getVariable1”; “get VARABLE2”

“PASSWORD execute reboot; PASSWORD get Variable1”; “get VARABLE2”

Note: Commands, variables and values are case sensitive.

List of basic execute commands

A list of basic commands which can be used in conjunction with the execute command are listed below:

“pdpcycle”, “pdpdown” and “pdpup” commands can have a profile number suffix ‘x’ added. Without the suffix specified, the command operates against the default profile configured on the profile list page of the Web-UI.

#	COMMAND NAME	DESCRIPTION
1	reboot	Immediately performs a soft reboot.
2	pdpcycle	Disconnects (if connected) and reconnects the data connection. If a profile number is selected in the command, try to disconnect/reconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect/reconnect the current active profile. Reports an error if no profile number is selected and there is no currently activated profile.
3	pdpdown	Disconnects the PDP. If a profile number is selected in the command, the router tries to disconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect the current active profile. Reports an error if no profile number is selected and there is no currently activated profile.
4	pdpup	Reconnects the PDP. If a profile number is selected in the command, the router tries to connect with the specified profile. If no profile number is selected, the router tries to connect to the last active profile. The gateway will check the currently activated profile and disconnect this profile before executing the command. The router reports an error if no profile number is selected and there is no stored last active profile number.
5	factorydefaults	Performs a factory reset on the router. Be aware that this command also clears the SMS white list on the router.
6	download	Performs a download and install of a Firmware Upgrade (.cdi), Config File (.tar.gz) or a help document (.pdf) file. If the file is a firmware image as in the case of a .cdi file, the router will apply the recovery image first and then the main firmware image. The download location is specified immediately after the command and may be from an HTTP or FTP source URL. If the file is a .tar.gz file, the router will apply the file as a configuration file update for the device and reboot afterwards. If the file is a .pdf, the router will assume this is a user guide document and save it to the router and make the file available for viewing via the help menu on the Web-UI. Note: If your download URL includes any space characters, please encode these prior to transmission according to RFC1738, for example: ftp://username:password@serveraddress/directory%20with%20spaces/filename.cdi Note: Authenticated FTP addresses may be used following the format as defined in RFC1738, for example: ftp://username:password@serveraddress/directory/filename.cdi
7	codconnect	Causes the router to activate the PDP context when the Connect on demand feature is enabled.
8	coddisconnect	Causes the router to de-activate the PDP context when the Connect on demand feature is enabled.
9	wakeup	This forces the default Data connection profile to connect if it is in a disconnected or waiting state. There are two circumstances in which this command may be useful; where the default profile is enabled but has been manually disconnected and if Connect on demand is enabled and the router is awaiting packet of interest. In both of these situations, the wakeup command will cause the default PDP context to activate.
10	ssh.genkeys	Instructs the router to generate new public SSH keys.
11	ssh.clearkeys	Instructs the router to clear the client public SSH key files.

Table 24 - List of basic SMS diagnostic commands

List of get/set commands

The following table is a partial list of get and set commands which may be performed via SMS.

COMMAND NAME	EXAMPLE	DESCRIPTION
get status	get status	Returns the Module firmware version, LAN IP Address, Network State, Network operator and RSSI.
get sessionhistory	get sessionhistory	Returns the time and date of recent sessions along with the total amount of data sent and received for each session.
set syslogserver	set syslogserver=123.45.67.89:514	Sets a remote syslog server IP or hostname and port.
set cod	set cod=1	Enables or disables Connect on demand.
get cod	get cod	Returns the enable/disable status of the Connect on demand feature.
get codstatus	get codstatus	Returns the connection status of the Connect on demand feature.
set coddialport	set coddialport=on,53	Sets the Connect on demand feature to connect only when traffic is received on the specified port.
get coddialport	get coddialport	Returns the Connect on demand port filter status and list or filtered ports.
set codonline	set codonline=20	Sets the router to stay online for at least X minutes when data activity is detected.
get codonline	get codonline	Returns the number of minutes the router is configured to stay online when data activity is detected.
set codminonline	set codminonline=10	Sets the router to stay online for a minimum of X minutes after connecting.
get codminonline	get codminonline	Returns the minimum number of minutes the router should stay online after connecting.
set codredial	set codredial=5	Sets the number of minutes that the router should not attempt to redial after hanging up.
get codredial	get codredial	Returns the number of minutes that the router is configured to not attempt to redial after hanging up.
set coddisconnect	set coddisconnect=0	Sets the number of minutes after which the router should disconnect regardless of traffic.
get coddisconnect	get coddisconnect	Returns the number of minutes the router is configured to disconnect regardless of traffic.
set codconnectreg	set codconnectreg=30	Sets the number of minutes that the router should regularly attempt to connect.
get codconnectreg	get codconnectreg	Returns the number of minutes that the router is configured to regularly attempt to connect.
set codrandomtime	set codrandomtime=3	Sets the number of minutes that the router should randomise the dial time by.
get codrandomtime	get codrandomtime	Returns the number of minutes that the router is configured to randomise the dial time by.
set codverbose	set codverbose=1	Sets verbose logging on or off.
get codverbose	get codverbose	Returns the status of verbose logging.
set codignore.icmp	set codignore.icmp=1	Sets the router to ignore ICMP packets triggering data activity detection.
get codignore.icmp	get codignore.icmp	Returns the status of the Ignore ICMP option.
set codignore.tcp	set codignore.tcp=1	Sets the router to ignore TCP packets triggering data activity detection.
get codignore.tcp	get codignore.tcp	Returns the status of the Ignore TCP option.
set codignore.udp	set codignore.udp=1	Sets the router to ignore UDP packets triggering data activity detection.
get codignore.udp	get codignore.udp	Returns the status of the Ignore UDP option.
set codignore.dns	set codignore.dns=1	Sets the router to ignore DNS traffic triggering data activity detection.
get codignore.dns	get codignore.dns	Returns the status of the Ignore DNS option.
set codignore.ntp	set codignore.ntp=1	Sets the router to ignore NTP traffic triggering data activity detection.
get codignore.ntp	get codignore.ntp	Returns the status of the Ignore NTP option.
set codignore.ncsi	set codignore.ncsi=1	Sets the router to ignore NCSI traffic triggering data activity detection.
get codignore.ncsi	get codignore.ncsi	Returns the status of the Ignore NCSI option.
get pppoe	get pppoe	Returns the PPPoE status, currently configured dial string and service name
set pppoe	set pppoe=1, telstra.internet, test	Sets the PPPoE status on, APN to telstra.internet, and service name to test.
get ledmode	get ledmode	Returns the status of the LED operation mode.
set ledmode	set ledmode=10	Sets the LED operation mode to be always on or to turn off after the specified number of minutes.
get ssh.proto	get ssh.proto	Returns the SSH protocol in use.
set ssh.proto	set ssh.proto=1,2	Sets the SSH Protocol to protocol 1, 2 or both (1,2).

get ssh.passauth	get ssh.passauth	Returns the status of the SSH Enable password authentication option.
set ssh.passauth	set ssh.passauth=1	Sets the SSH Enable password authentication option on or off.
get.ssh.keyauth	get.ssh.keyauth	Returns the status of the SSH Enable key authentication option.
set.ssh.keyauth	set.ssh.keyauth=1	Sets the SSH Enable key authentication option on or off.

Table 25 - List of get/set commands

List of basic RDB variables

The following table lists valid variables where "x" is a profile number (1-6). If no profile is specified, variables are read from or written to for the current active profile. If a profile is specified, variables are read from or written to for the specified profile number ('x').

#	RDB VARIABLE NAME	SMS VARIABLE NAME	READ/ WRITE	DESCRIPTION	EXAMPLE VALUE
0	link.profile.1.enable link.profile.1.apn link.profile.1.user link.profile.1.pass link.profile.1.auth_type link.profile.1.iplocal link.profile.1.status	profile	RW	Profile	Read: (profile no,atd#xxx,user,pass,auth,iplocal,status) 1,atd#777,username,password, chap,202.44.185.111,up Write: (atd#xxx, user, pass,auth) atd#777,username,password
2	link.profile.1.user	username	RW	profile username	Guest, could also return "null"
3	link.profile.1.pass	password	RW	profile password	Guest, could also return "null"
4	link.profile.1.auth_type	authtype	RW	Authentication type	"pap" or"chap"
5	link.profile.1.iplocal	wanip	R	WAN IP address	202.44.185.111
6	wwan.0.radio.information.signal_strength	rssi	R	signal strength	-65 dBm
7	wwan.0.meid	meid	R	MEID number	0x00A1000021D003BB
8	statistics.usage_current	usage	R	mobile data usage of current session	"Rx 500 bytes, Tx 1024 bytes, Total 1524 bytes" or "Rx 0 byte, Tx 0 byte, Total 0 byte" when wwan down
9	statistics.usage_current	wanuptime	R	Up time of current mobile session	1 days 02:30:12 or 0 days 00:00:00 when wwan down
10	/proc/uptime	deviceuptime	R	Device up time	1 days 02:30:12
11	wwan.0.system_network_status.current_band	band	R	Current frequency channel & band	CH 426 PCS B Band

Table 26 - List of basic SMS diagnostics RDB variables

SMS diagnostics examples

The examples below demonstrate various combinations of supported commands. This is not an exhaustive list and serves as an example of possibilities only.

DESCRIPTION	AUTHENTICATION	INPUT EXAMPLE
Send SMS to change the data connection username	Not required	set username='NetComm'
	Required	PASSWORD set username= "NetComm"
Send SMS to change the data connection password	Not required	set password= `NetComm`
	Required	PASSWORD set password= `NetComm`
Send SMS to change the data connection authentication	Not required	set authtype= 'pap'
	Required	PASSWORD set authtype = pap
Send SMS to reboot	Not required	execute reboot
	Required	PASSWORD execute reboot
Send SMS to check the WAN IP address	Not required	get wanip
	Required	PASSWORD get wanip
Send SMS to check the mobile signal strength	Not required	get rssi
	Required	PASSWORD get rssi
Send SMS to check the MEID number	Not required	Get meid
	Required	PASSWORD get meid
Send SMS to check the current band	Not required	get band
	Required	PASSWORD get band
Send SMS to Disconnect (if connected) and reconnect the data connection	Not required	execute pdpcycle
	Required	PASSWORD execute pdpcycle
Send SMS to disconnect the data connection	Not required	execute pdpdown
	Required	PASSWORD execute pdpdown
Send SMS to connect the data connection	Not required	execute pdpup
	Required	PASSWORD execute pdpup
Send multiple get command	Not required	get wanip; get rssi
	Required	PASSWORD get wanip; get rssi
Send multiple set command	Not required	set ssh.genkeys=1; set username=test; set auth=pap
	Required	PASSWORD set ssh.genkeys=1; set username=test; set auth=pap
Send SMS to reset to factory default settings	Not required	execute factorydefaults
	Required	PASSWORD execute factorydefaults
Send SMS to retrieve status of router	Not required	get status
	Required	PASSWORD get status
Send SMS to retrieve the history of the session, including start time, end time and total data usage	Not required	get sessionhistory
	Required	PASSWORD get sessionhistory
Send SMS to configure the router to send syslog to a remote syslog server	Not required	set syslogserver=123.209.5.68
	Required	PASSWORD set syslogserver=123.209.5.68
Send SMS to wake up the router, turn on the default gateway and trigger the 'connect on demand' profile if in waiting state.	Not required	execute wakeup
	Required	PASSWORD execute wakeup
Send SMS to perform firmware upgrade when firmware is located on HTTP server	Not required	execute download http://download.com:8080/firmware_image.cdi execute download http://download.com:8080/firmware_image_r.cdi
	Required	PASSWORD execute download http://download.com:8080/firmware_image.cdi PASSWORD execute download http://download.com:8080/firmware_image_r.cdi
Send SMS to perform firmware upgrade when firmware is located	Not required	execute download ftp://username:password@download.com/firmware_image.cdi

on FTP server		execute download ftp://username:password@ download.com/firmware_image_r.cdi
	Required	PASSWORD execute download ftp://username:password@ download.com/firmware_image.cdi PASSWORD execute download ftp://username:password@ download.com/firmware_image_r.cdi
Send SMS to download and install IPK package located on HTTP server	Not required	execute download http://download.com:8080/package.ipk
	Required	PASSWORD execute download http://download.com:8080/package.ipk
Send SMS to download and install IPK package located on FTP server	Not required	execute download ftp://username:password@ download.com:8080/package.ipk
	Required	PASSWORD execute download ftp://username:password@ download.com:8080/package.ipk
Send SMS to turn off PPPoE	Not required	set pppoe=0
	Required	PASSWORD set pppoe=0
Send SMS to retrieve the PPPoE status, currently configured dial string and service name	Not required	get pppoe
	Required	PASSWORD get pppoe
Send SMS to set the LED mode timeout to 10 minutes	Not required	set ledmode=10
	Required	PASSWORD set ledmode=10
Send SMS to retrieve the current LED mode	Not required	get ledmode
	Required	PASSWORD get ledmode
Retrieve current SSH protocol	Not required	get ssh.proto
	Required	PASSWORD get ssh.proto
Select SSH protocol	Not required	set ssh.proto=1
	Required	PASSWORD set ssh.proto=1
Retrieve password authentication status	Not required	get ssh.passauth
	Required	PASSWORD get.ssh.passauth
Enable/disable password authentication on host	Not required	set ssh.passauth=1 or set ssh.passauth=0
	Required	PASSWORD set ssh.passauth=1 or PASSWORD set ssh.passauth=0
Generate set of public/private keys on the host	Not required	execute ssh.genkeys
	Required	PASSWORD execute ssh.genkeys
Clear client public keys stored on host	Not required	execute ssh.clearkeys
	Required	PASSWORD execute ssh.clearkeys

Table 27 - SMS diagnostics example commands

System

Log

The Log pages are used to display or download the System log and IPSec logs on the router.

System log

The System Log enables you to troubleshoot any issues you may be experiencing with your NWL-15 router. To access the System Log page, click on the **System** menu. The System Log is displayed.

Log File

Use the **Display level** drop-down list to select a message level to be displayed. The message levels are described in the table below.

To download the System log for offline viewing, right-click the **Download** button and choose **Save as..** to save the file. To clear the System log, click the **Clear** button. The downloaded log file is in Linux text format with carriage return (CR) only at the end of a line, therefore in order to be displayed correctly with new lines shown, it is recommended to use a text file viewer which displays this format correctly (e.g. Notepad++).

Log data is stored in RAM and therefore, when the unit loses power or is rebooted, it will lose any log information stored in RAM. To ensure that log information is accessible between reboots of the router there are two options:

1. Enable the **Log to file** option
2. Use a remote syslog server

Enable log to file

When the router is configured to log to a file, the log data is stored in flash memory, making it accessible after a reboot of the router. Up to 512kb of log data will be stored before it is overwritten by new log data. Flash memory has a finite number of program-erase operations that it may perform to the blocks of memory. While this number of program-erase operations is quite large, we recommend that you do not enable this option for anything other than debugging to avoid excessive wear on the memory.

Use a remote syslog server

The router can be configured to output log data to a remote syslog server. This is an application running on a remote computer which accepts and displays the log data. Most syslog servers can also save the log data to a file on the computer on which it is running allowing you to ensure that no log data is lost between reboots.

To configure the NWL-15 router to output log data to a remote syslog server:

1. Click on the **System** menu from the top menu bar. The System log item is displayed.
2. Under the **Remote syslog server** section, enter the IP address or hostname of the syslog server in the **IP / Hostname [PORT]** field. You can also specify the port number after the IP or hostname by entering a semi-colon and then the port number e.g. 192.168.1.102:514. If you do not specify a port number, the router will use the default UDP port 514.
3. Click the **Save** button to save the configuration.

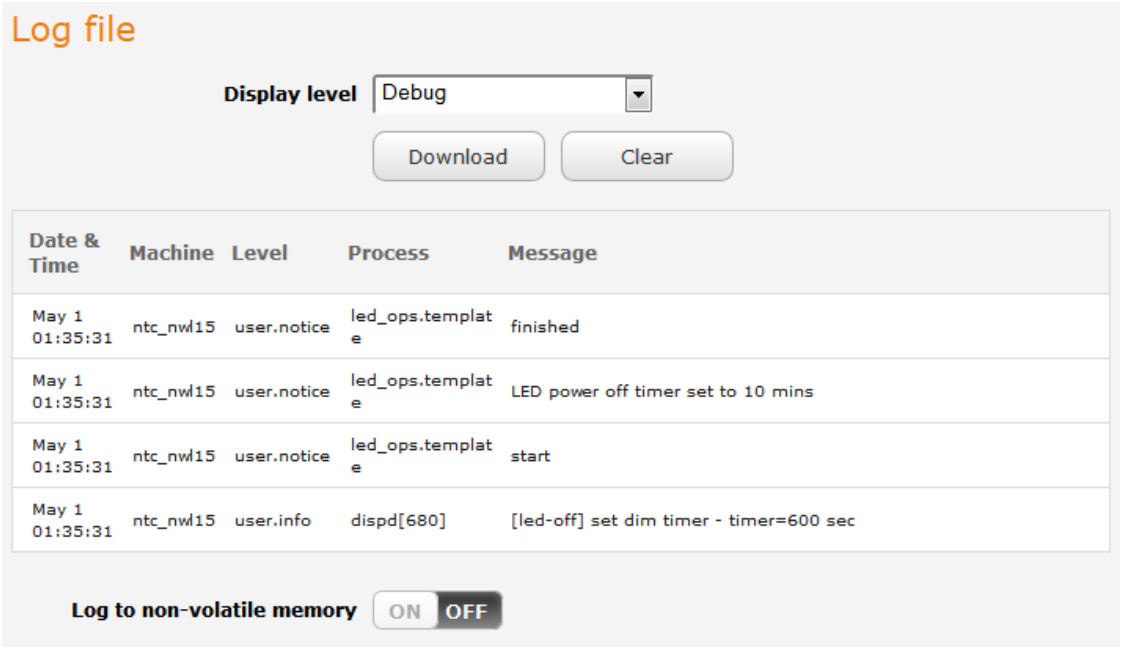


Figure 108 - System log

ITEM	DEFINITION
Debug	Show extended system log messages with full debugging level details.
Info	Show informational messages only.
Notice	Show normal system logging information.
Error	Show error condition messages only.

Table 28 - System log detail levels

IPSec log

The IPSec log section provides the ability for you to download the log for the IPSec VPN function. This can assist in troubleshooting any problems you may have with the IPSec VPN.

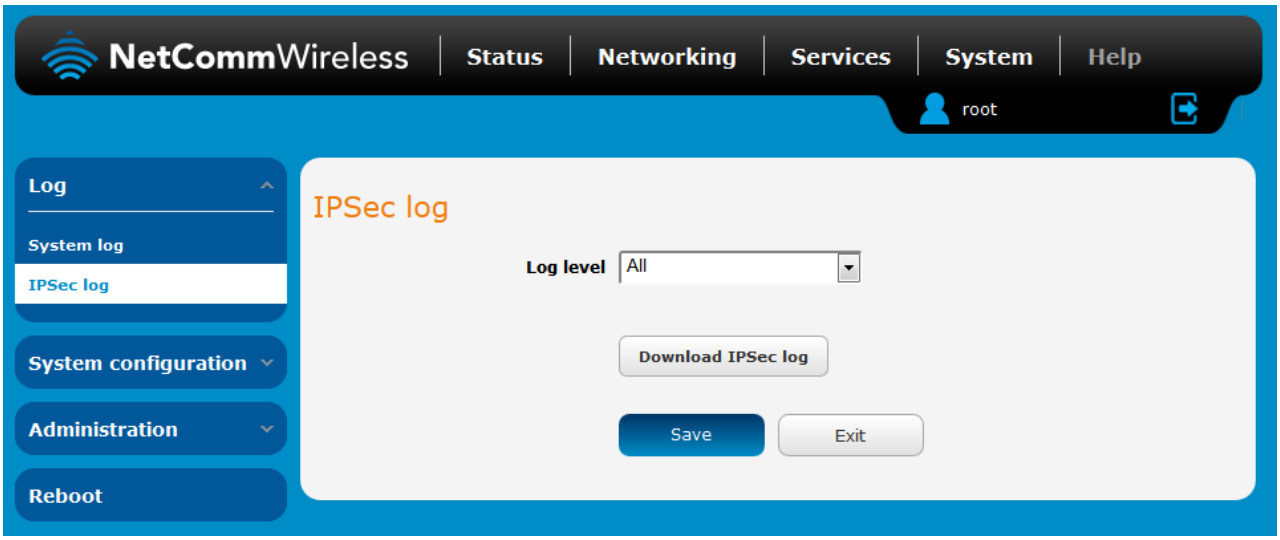


Figure 109 - IPSec log

Use the **Log level** drop down list to specify the type of detail you want to capture in the log and then click the **Save** button. When you change the logging level, any active IPSec VPN tunnels will be disconnected as a change in logging level requires the IPSec service to be restarted.

To download the IPSec log, click the **IPSec log download** button and you will be prompted to save the file.

System configuration

Settings backup and restore

The settings backup and restore page is used to backup or restore the router's configuration or to reset it to factory defaults. In order to view the settings page you must be logged into the web user interface as **root** using the password **admin**. The backup and restore functions can be used to easily configure a large number of NWL-15 router by configuring one router with your desired settings, backing them up to a file and then restoring that file to multiple NWL-15 routers.

Figure 110 – Settings backup and restore

Back up your router's configuration

Log in to the web configuration interface, click on the **System** menu and select **Settings backup and restore**.

If you want to password protect your backup configuration files, enter your password in the fields under **Save a copy of current settings** and click on **Save**. If you don't want to password protect your files, just click on **Save**. The router will then prompt you to select a location to save the settings file.

Note: The following conditions apply:-

- It is NOT possible to edit the contents of the file downloaded; if you modify the contents of the configuration file in any way you will not be able to restore it later.
- You may change the name of the file if you wish but the filename extension must remain as ".cfg.tar.gz"
- Backups protected with a password cannot be restored remotely.

Restore your backup configuration

1. In the web configuration interface click on the **System** menu and select **Settings backup and restore**.
2. From the **Restore saved settings** section, click on **Browse** or **Choose a File** and select the backup configuration file on your computer.
3. Click **Restore** to copy the settings to the new NWL-15 router. The router will apply these settings and inform you it will reboot - click on **OK**.

Restoring the router's factory default configuration

Click the **Restore Defaults** button to restore the factory default configuration. The router asks you to confirm that you wish to restore factory default settings. If you wish to continue with the restoring of factory defaults, click **OK**.

Note: All current settings on the router will be lost when performing a restore of factory default settings. The device IP address will change to 192.168.1.1 and the default username **root** and default password **admin** will be configured.

Upload

To access the Upload page, click on the **System** menu, then **System Configuration** and then **Upload**.

The Upload page allows you to upload firmware files, HTTPS certificates or user created application packages to the NWL-15 router. When firmware files have been uploaded, they can also be installed from this page. PDF files, such as this user guide may also be uploaded for access on the router's help page.

For more information on application development, contact NetComm Wireless about our Software Development Kit.

Figure 111 - Upload page

Updating the Firmware

The firmware update process involves first updating the recovery image firmware and then updating the main firmware image.

Note: In order to perform an update, you must be logged into the router with the root manager account (see the Advanced configuration section for more details).

To update the NWL-15 router firmware:

1. Power on the router as described in the Powering the router section.
2. Log in to the router with the root user account (See the Installing the router section for details)
3. Select the System item from the top menu bar, select the System configuration item from the menu on the left and then select the Upload menu item.
4. Under the File uploads section, click the Choose a File button. Locate the recovery firmware image file on your computer and click Open. The recovery image is named ntc_nwl15_x.xx.xx.x_r.cdi while the main system firmware image is named vdf_nwl15_x.xx.xx.x.cdi.
5. Click the Upload button. The firmware image is uploaded to the storage on the router.

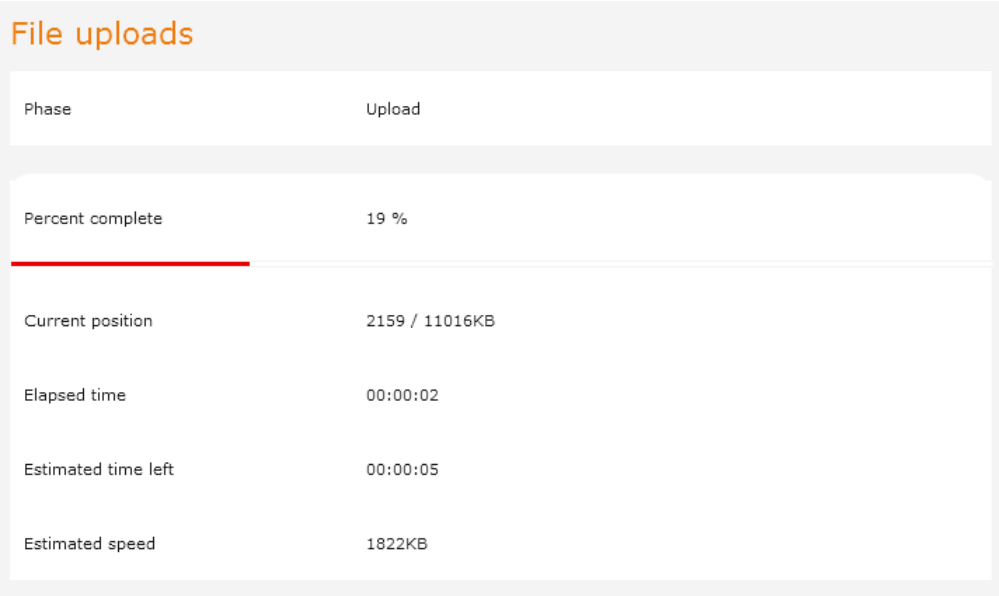


Figure 112 - File upload

6. Repeat steps 4 and 5 for the main system firmware image.
7. The uploaded firmware images are listed in the **Uploaded files** section. Click the **Install** link next to the recovery image to begin installing the recovery firmware image and then click **OK** on the confirmation window that appears.

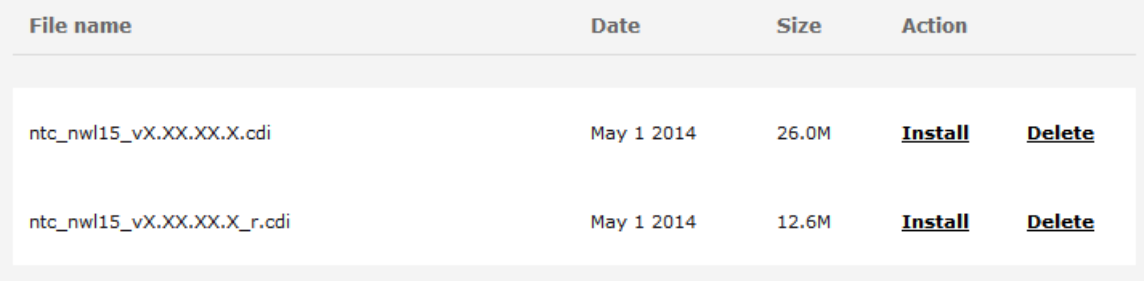


Figure 113 - Uploaded files

8. The recovery firmware image is flashed and when it is complete, the router displays "The firmware update was successful" and returns to the main Upload screen.

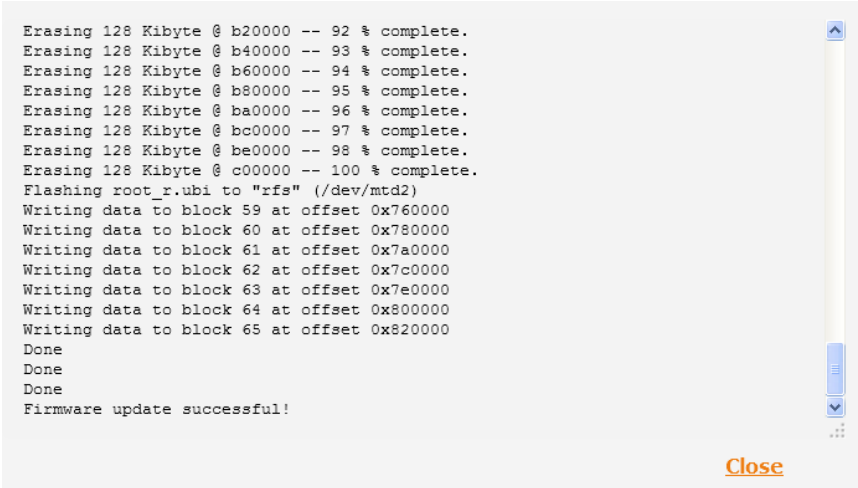
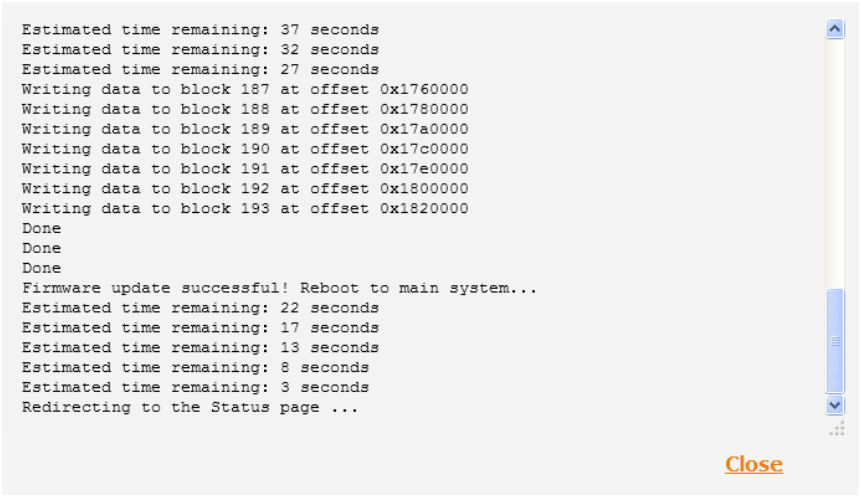

Erasing 128 Kibyte @ b20000 -- 92 % complete.
Erasing 128 Kibyte @ b40000 -- 93 % complete.
Erasing 128 Kibyte @ b60000 -- 94 % complete.
Erasing 128 Kibyte @ b80000 -- 95 % complete.
Erasing 128 Kibyte @ ba0000 -- 96 % complete.
Erasing 128 Kibyte @ bc0000 -- 97 % complete.
Erasing 128 Kibyte @ be0000 -- 98 % complete.
Erasing 128 Kibyte @ c00000 -- 100 % complete.
Flashing root_r.ubi to "rfs" (/dev/mtd2)
Writing data to block 59 at offset 0x760000
Writing data to block 60 at offset 0x780000
Writing data to block 61 at offset 0x7a0000
Writing data to block 62 at offset 0x7c0000
Writing data to block 63 at offset 0x7e0000
Writing data to block 64 at offset 0x800000
Writing data to block 65 at offset 0x820000
Done
Done
Done
Firmware update successful!
Close

Figure 114 - Recovery firmware flash process

9. Click the **Install** link to the right of the main firmware image you uploaded and then click **OK** to confirm that you want to continue with the installation.

Note: Do not remove the power when the router's LEDs are flashing as this is when the firmware update is in process.

10. The installation is complete when the countdown reaches zero. The router redirects you to the Status page.


Estimated time remaining: 37 seconds
Estimated time remaining: 32 seconds
Estimated time remaining: 27 seconds
Writing data to block 187 at offset 0x1760000
Writing data to block 188 at offset 0x1780000
Writing data to block 189 at offset 0x17a0000
Writing data to block 190 at offset 0x17c0000
Writing data to block 191 at offset 0x17e0000
Writing data to block 192 at offset 0x1800000
Writing data to block 193 at offset 0x1820000
Done
Done
Done
Firmware update successful! Reboot to main system...
Estimated time remaining: 22 seconds
Estimated time remaining: 17 seconds
Estimated time remaining: 13 seconds
Estimated time remaining: 8 seconds
Estimated time remaining: 3 seconds
Redirecting to the Status page ...
Close

11. Hold down the reset button on the router for 15-20 seconds to reboot and restore the factory default settings of the router. See the Restoring factory default settings section for more information.

Package Manager

The Package Manager page is used to provide details of any user installed packages on the router and allow them to be uninstalled.

For more information on application development, contact NetComm Wireless about our Software Development Kit.

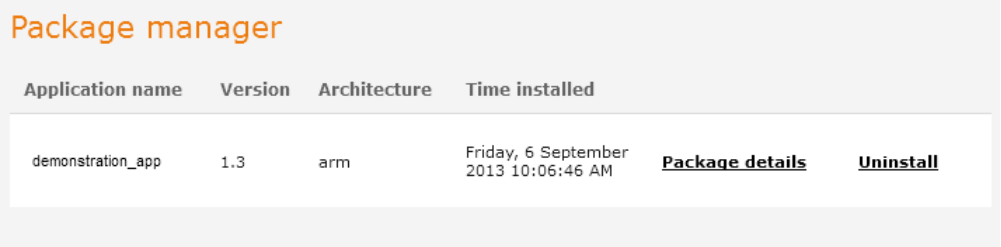


Figure 115 – Software applications manager

The Application name, Version number of the application, the architecture type and time of installation are all displayed. Clicking the Package details link will display a pop-up window with further details of the package.

To uninstall any software applications, click the Uninstall link.

Administration settings

To access the Administration Settings page, click on the System menu then the Administration menu on the left and then click on Administration Settings.

The Administration settings page is used to enable or disable protocols used for remote access and configure the passwords for the user accounts used to log in to the router.

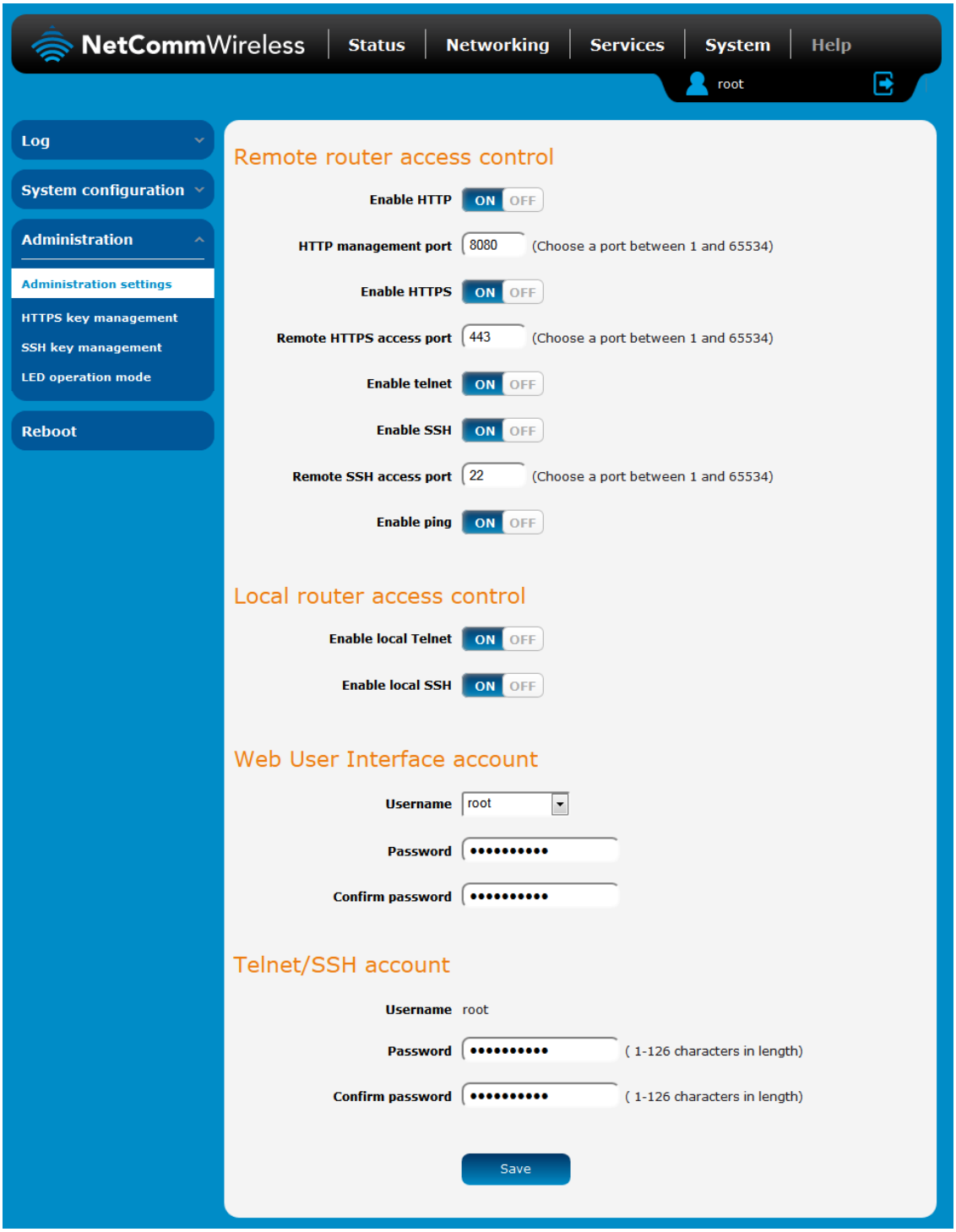


Figure 116 - Administration page

OPTION	DEFINITION
Remote router access control	
Enable HTTP	Enable or disable remote HTTP access to the router. You can also set the port you would like remote HTTP access to be available on.
HTTP management port	Enter a port number between 1 and 65534 to use when accessing the router remotely.
Enable HTTPS	Enable or disable remote HTTPS access to the router using a secure connection.
Remote HTTPS access port	Enter a port number between 1 and 65534 to use when accessing the router remotely over a secure HTTPS connection.
Enable Telnet	Enable or disable remote telnet (command line) access to the router.
Enable SSH	Enable or disable Secure Shell on the router.
Remote SSH Access Port	Enter the port number for remote SSH access. Must be a port number between 1 and 65534.
Enable Ping	Enable or disable remote ping responses on the WWAN connection.
Local router access control	
Enable local Telnet	When turned on, this enables you to telnet to the router when connected locally.
Enable local SSH	When turned on, this enables you to SSH to the router when connected locally.
Web User Interface account	
Username	Use the drop down list to select the **root** or **admin** account to change its web user interface password.
Password	Enter the desired web user interface password.
Confirm password	Re-enter the desired web user interface password.
Telnet/SSH account	
Username	Displays the Telnet/SSH.username. This may not be changed.
Password	Enter the desired Telnet/SSH password.
Confirm password	Re-enter the desired Telnet/SSH password.

Table 29 - Administration configuration options

To access the router's configuration pages remotely:

1. Open a new browser window and navigate to the WAN IP address and assigned port number of the router, for example http://123.209.130.249:8080

Note: You can find the router's WAN IP address by clicking on the "Status" menu. The WWAN IP field in the WWAN Connection Status section shows the router's WAN IP address.

2. Enter the username and password to login to the router and click **Log in**.

Note: To perform functions like Firmware upgrade, device configuration backup and to restore and reset the router to factory defaults, you must be logged in with the root manager account.

HTTPS Key Management

What is HTTP Secure?

HTTP Secure or HTTPS is the use of the HTTP protocol over an SSL/TLS protocol. It is used primarily to protect against eavesdropping of communication between a web browser and the web site to which it is connected. This is especially important when you wish to have a secure connection over a public network such as the internet. HTTPS connections are secured through the use of certificates issued by trusted certificate authorities such as VeriSign. When a web browser makes a connection attempt to a secured web site, a digital certificate is sent to the browser so that it can verify the authenticity of the site using a built-in list of trusted certificate authorities.

There are two main differences between how HTTPS and HTTP connections work:

1. HTTPS uses port 443 while HTTP uses port 80 by default.
2. Over an HTTPS connection, all data sent and received is encrypted with SSL while over an HTTP connection, all data is sent unencrypted.

The encryption is achieved through the use of a pair of public and private keys on both sides of the connection. In cryptography, a key refers to a numerical value used by an algorithm to alter information (encrypt it), making the information secure and visible only to those who have the corresponding key to recover (decrypt) the information. The public key is used to encrypt information and can be distributed freely. The private key is used to decrypt information and must be secret by its owner.

Each NWL-15 router contains a self-signed digital certificate which is identical on all NWL-15 routers. For a greater level of security, the router also supports generating your own unique key. Additionally, you may use third party software to generate your own self-signed digital certificate or purchase a signed certificate from a trusted certificate authority and then upload those certificates to the router.

Generating your own self-signed certificate

To generate your own self-signed certificate:

1. Click the **Services** item from the top menu bar, then **HTTPS** from the side menu bar.
2. Enter the certificate details using the appropriate fields. Each field must be completed in order to generate a certificate.

Figure 117 - Generate self signed HTTPS certificate

Note: The **Country** field must contain a code for the desired country from the list below.

CODE	COUNTRY	CODE	COUNTRY	CODE	COUNTRY	CODE	COUNTRY
AX	Åland Islands	ER	Eritrea	LS	Lesotho	SA	Saudi Arabia
AD	Andorra	ES	Spain	LT	Lithuania	SB	Solomon Islands
AE	United Arab Emirates	ET	Ethiopia	LU	Luxembourg	SC	Seychelles
AF	Afghanistan	FI	Finland	LV	Latvia	SE	Sweden
AG	Antigua and Barbuda	FJ	Fiji	LY	Libya	SG	Singapore
AI	Anguilla	FK	Falkland Islands (Malvinas)	MA	Morocco	SH	St. Helena
AL	Albania	FM	Micronesia	MC	Monaco	SI	Slovenia
AM	Armenia	FO	Faroe Islands	MD	Moldova	SJ	Svalbard and Jan Mayen
AN	Netherlands Antilles	FR	France	ME	Montenegro	SK	Slovak Republic
AO	Angola	FX	France, Metropolitan	MG	Madagascar	SL	Sierra Leone
AQ	Antarctica	GA	Gabon	MH	Marshall Islands	SM	San Marino
AR	Argentina	GB	Great Britain (UK)	MK	Macedonia	SN	Senegal
AS	American Samoa	GD	Grenada	ML	Mali	SR	Suriname
AT	Austria	GE	Georgia	MM	Myanmar	ST	Sao Tome and Principe
AU	Australia	GF	French Guiana	MN	Mongolia	SU	USSR (former)
AW	Aruba	GG	Guernsey	MO	Macau	SV	El Salvador
AZ	Azerbaijan	GH	Ghana	MP	Northern Mariana	SZ	Swaziland
BA	Bosnia and Herzegovina	GI	Gibraltar	MQ	Martinique	TC	Turks and Caicos Islands
BB	Barbados	GL	Greenland	MR	Mauritania	TD	Chad
BD	Bangladesh	GM	Gambia	MS	Montserrat	TF	French Southern Territories
BE	Belgium	GN	Guinea	MT	Malta	TG	Togo
BF	Burkina Faso	GP	Guadeloupe	MU	Mauritius	TH	Thailand
BG	Bulgaria	GQ	Equatorial Guinea	MV	Maldives	TJ	Tajikistan
BH	Bahrain	GR	Greece	MW	Malawi	TK	Tokelau
BI	Burundi	GS	S. Georgia and S. Sandwich	MX	Mexico	TM	Turkmenistan
BJ	Benin	GT	Guatemala	MY	Malaysia	TN	Tunisia
BM	Bermuda	GU	Guam	MZ	Mozambique	TO	Tonga
BN	Brunei Darussalam	GW	Guinea-Bissau	NA	Namibia	TP	East Timor
BO	Bolivia	GY	Guyana	NC	New Caledonia	TR	Turkey
BR	Brazil	HK	Hong Kong	NE	Niger	TT	Trinidad and Tobago
BS	Bahamas	HM	Heard and McDonald Islands	NF	Norfolk Island	TV	Tuvalu
BT	Bhutan	HN	Honduras	NG	Nigeria	TW	Taiwan
BV	Bouvet Island	HR	Croatia (Hrvatska)	NI	Nicaragua	TZ	Tanzania
BW	Botswana	HT	Haiti	NL	Netherlands	UA	Ukraine
BZ	Belize	HU	Hungary	NO	Norway	UG	Uganda
CA	Canada	ID	Indonesia	NP	Nepal	UM	US Minor Outlying Islands
CC	Cocos (Keeling) Islands	IE	Ireland	NR	Nauru	US	United States
CF	Central African Republic	IL	Israel	NT	Neutral Zone	UY	Uruguay
CH	Switzerland	IM	Isle of Man	NU	Niue	UZ	Uzbekistan
CI	Cote D'Ivoire (Ivory	IN	India	NZ	New Zealand	VA	Vatican City State (Holy See)
CK	Cook Islands	IO	British Indian Ocean Territory	OM	Oman	VC	Saint Vincent and the
CL	Chile	IS	Iceland	PA	Panama	VE	Venezuela
CM	Cameroon	IT	Italy	PE	Peru	VG	Virgin Islands (British)
CN	China	JE	Jersey	PF	French Polynesia	VI	Virgin Islands (U.S.)
CO	Colombia	JM	Jamaica	PG	Papua New Guinea	VN	Viet Nam
CR	Costa Rica	JO	Jordan	PH	Philippines	VU	Vanuatu
CS	Czechoslovakia (former)	JP	Japan	PK	Pakistan	WF	Wallis and Futuna Islands
CV	Cape Verde	KE	Kenya	PL	Poland	WS	Samoa
CX	Christmas Island	KG	Kyrgyzstan	PM	St. Pierre and Miquelon	YE	Yemen
CY	Cyprus	KH	Cambodia	PN	Pitcairn	YT	Mayotte
CZ	Czech Republic	KI	Kiribati	PR	Puerto Rico	ZA	South Africa
DE	Germany	KM	Comoros	PS	Palestinian Territory	ZM	Zambia
DJ	Djibouti	KN	Saint Kitts and Nevis	PT	Portugal	COM	US Commercial
DK	Denmark	KR	Korea (South)	PW	Palau	EDU	US Educational
DM	Dominica	KW	Kuwait	PY	Paraguay	GOV	US Government
DO	Dominican Republic	KY	Cayman Islands	QA	Qatar	INT	International
DZ	Algeria	KZ	Kazakhstan	RE	Reunion	MIL	US Military
EC	Ecuador	LA	Laos	RO	Romania	NET	Network
EE	Estonia	LC	Saint Lucia	RS	Serbia	ORG	Non-Profit Organization
EG	Egypt	LI	Liechtenstein	RU	Russian Federation	ARPA	Old style Arpanet
EH	Western Sahara	LK	Sri Lanka	RW	Rwanda		

3. When you have entered all the required details, press the **Generate** button. The certificate takes several minutes to generate. When the certificate has been generated, you are informed that it has been successfully generated and installed. The web server on the router restarts and you are logged out of the router. Click **OK** to be taken back to the login screen.

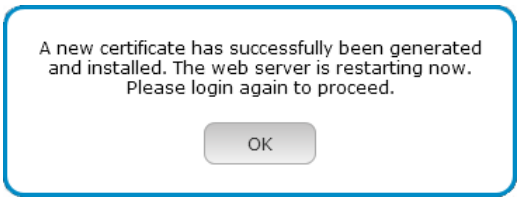

A new certificate has successfully been generated and installed. The web server is restarting now. Please login again to proceed.
OK

Figure 118 - New certificate successfully generated message

SSH key management

Secure Shell (SSH) is UNIX-based command interface and network protocol used to gain secure access to a remote computer, execute commands on a remote machine or to transfer files between machines. It was designed as a replacement for Telnet and other insecure remote shell protocols which send information, including passwords, as plain text.

SSH uses RSA public key cryptography for both connection and authentication. Two common ways of using SSH are:

- Use automatically generated public-private key pairs to encrypt the network connection and then use password authentication to log on.
- Use a manually generated public-private key pair to perform the authentication and allow users or programs to log in without using a password.

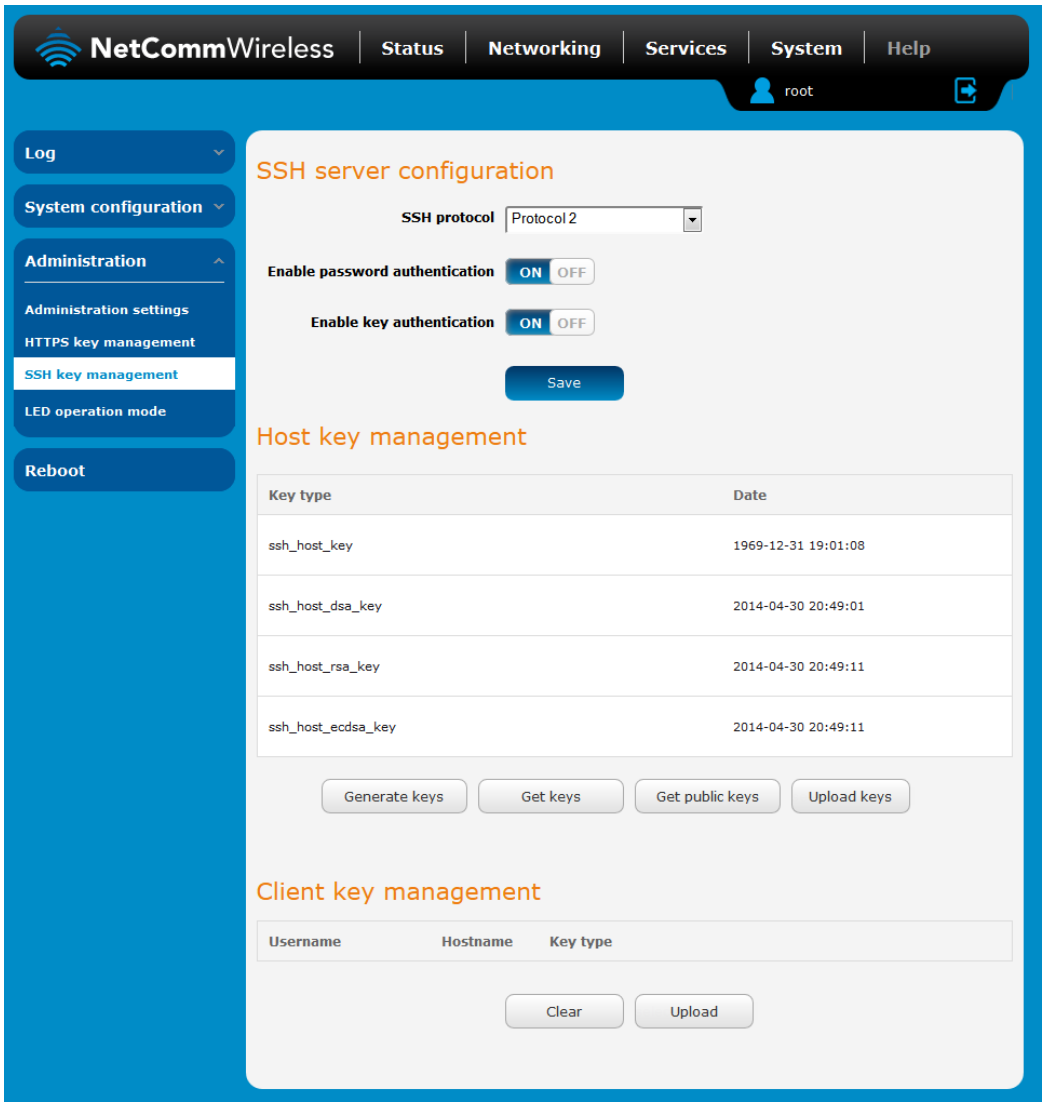


Figure 119 - SSH Server Configuration

SSH server configuration

To configure the SSH server settings:

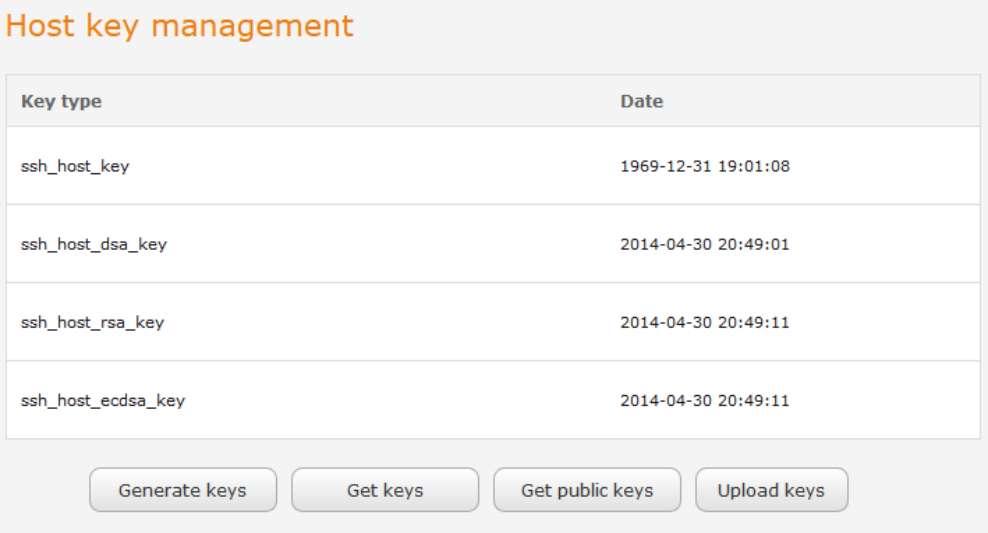
1. Use the SSH Protocol drop down list to select the protocol that you want to use. Protocol 2 is more recent and is considered more secure.
2. Select the types of authentication you want to use by clicking the Enable Password Authentication and Enable key Authentication toggle keys on or off. Note that you may have both authentication methods on but you may not turn them both off.
3. Click the Save button to confirm your settings.

Host key management

SSH keys provide a means of identification using public key cryptography and challenge response authentication. This means that a secure connection can be established without transmitting a password, thereby greatly reducing the threat of someone eavesdropping and guessing the correct credentials.

SSH Keys always come in pairs with one being a public key and the other a private key. The public key may be shared with any server to which you want to connect. When a connection request is made, the server uses the public key to encrypt a challenge (a coded message) to which the correct response must be given. Only the private key can decrypt this challenge and produce the correct response. For this reason, the private key should not be shared with those who you do not wish to give authorization.

The Host Key Management section displays the current public keys on the router and their date and timestamp. These public keys are provided in different formats, including DSA, RSA and ECDSA. Each format has advantages and disadvantages in terms of signature generation speed, validation speed and encryption/decryption speed. There are also compatibility concerns to consider with older clients when using ECDSA, for example.



Generating new keys

The complete set of keys can be re-generated by selecting the **Generate keys** button. This key generation process takes approximately 30 seconds to complete.

Downloading keys

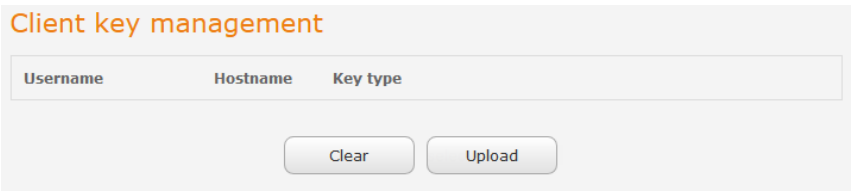
The **Get keys** button allows you to download the complete set of public and private keys while the **Get public keys** button will download only the set of public keys.

Uploading your own key files

Click the Upload keys button to upload your own public key to the router.

Client key management

The Client Key Management section is used for uploading the public key file of clients. To upload a client public key, click the **Upload** button, browse to the file and click **Open**.



When the file is uploaded, it is examined for validity. If the key file is not a valid public key, it will not be uploaded.

LED operation mode

The 7 front LED indicators may be turned off after a timeout period for aesthetic or power saving reasons. To access the LED Operation Mode page, click the **System** menu, then **Administration** on the left and finally select **LED Operation Mode**.

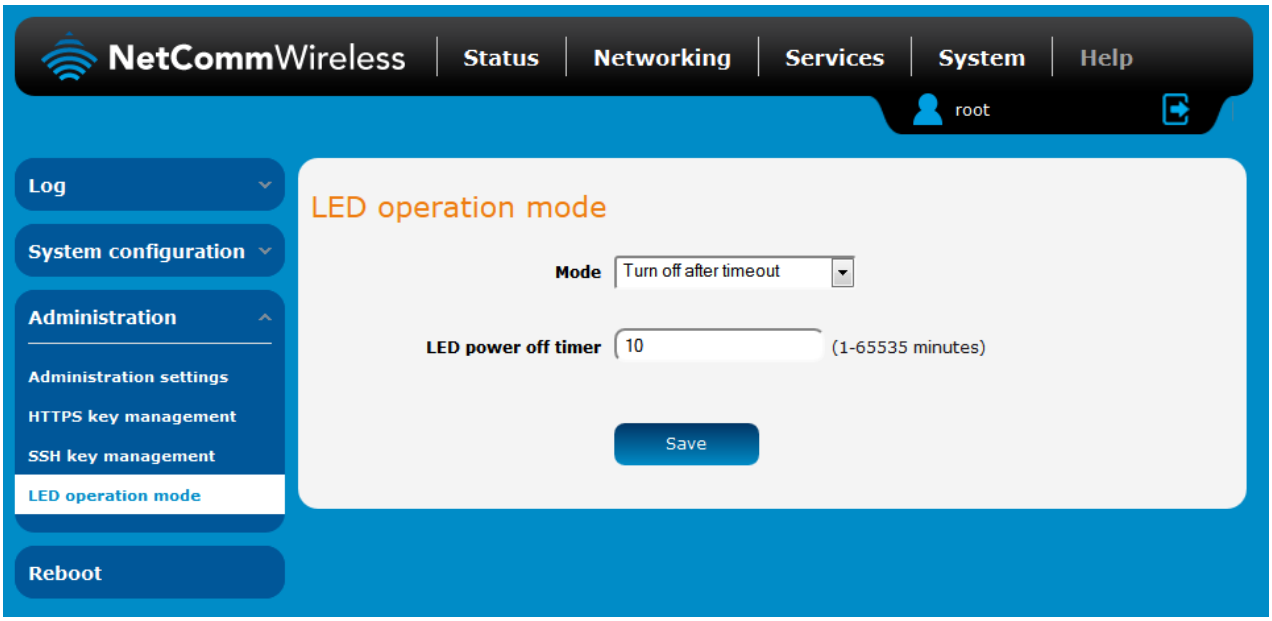


Figure 120 - LED Operation Mode

The **Mode** drop down list sets the operation mode of the LEDs on the front panel of the router. To set the lights to operate at all times, set this to Always on. To set the lights to turn off after a specified period, select **Turn off after timeout**. When configured to turn off after timeout, use the **LED power off timer** field to specify the time in minutes to wait before turning off the LED indicators. The LED power off timer must be an integer between 1 and 65535.

The wait period begins from the time the **Save** button is clicked. When the wait period expires, the LEDs will turn off. If the router is rebooted, the LED power off timer is reset. The router will boot up and wait for the configured time before turning off again.

Reboot

The reboot option in the System section performs a soft reboot of the router. This can be useful if you have made configuration changes you want to implement.

To reboot the router:

1. Click the **System** menu item from the top menu bar.
2. Click the **Reboot** button from the menu on the left side of the screen.

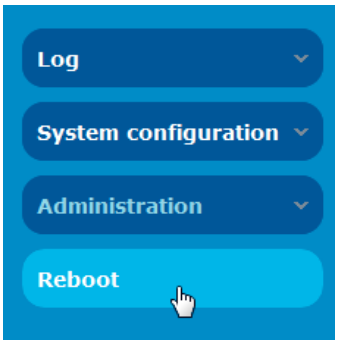


Figure 121 - Reboot menu option

3. The router displays a warning that you are about to perform a reboot. If you wish to proceed, click the **Reboot** button then click **OK** on the confirmation window which appears.

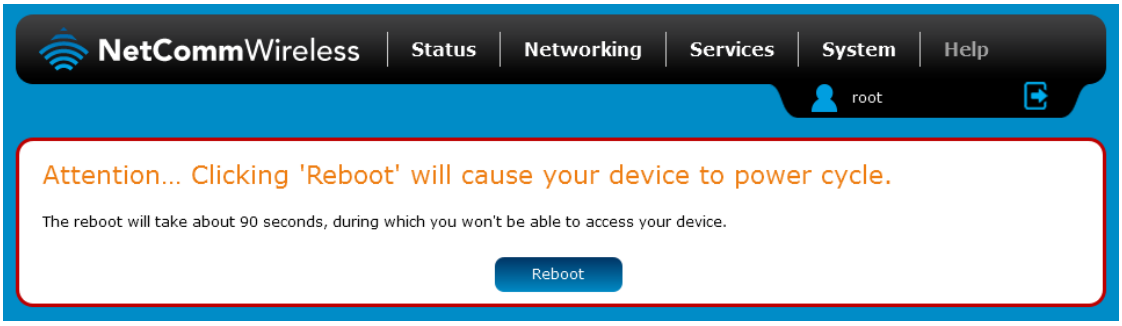


Figure 122 - Reboot confirmation

Note: It can take up to 2 minutes for the router to reboot.

Logging out

To log out of the router, click the icon at the top right corner of the web user interface.

Appendix A: Tables

Table 1 - Document Revision History 2
Table 2 - Device Dimensions....8
Table 3 - LED Indicators 9
Table 4 - Signal strength LED descriptions....10
Table 5 - Ethernet port LED indicators description....10
Table 6 – Interfaces 11
Table 7 - Locking power block pin outs....17
Table 8 - Average power consumption figures....18
Table 9 - Management account login details 19
Table 10 - Status page item details....22
Table 11 - Data connection item details 24
Table 12 - Connect on demand - Connect and disconnect timers descriptions....30
Table 13 - Band selection options....32
Table 14 - Current MAC / IP / Port filtering rules in effect 46
Table 15 - IPSec Configuration Items 49
Table 16 - Modem emulator options 68
Table 17 - Mobile Station Based Assisted GPS configuration options 78
Table 18 - Odometer configuration options 79
Table 19 - IO configuration options 80
Table 20 - IO configuration options 81
Table 21 - SMS Setup Settings....87
Table 22 - Inbox/Outbox icons....89
Table 23 - SMS Diagnostic Command Syntax....94
Table 24 - List of basic SMS diagnostic commands 95
Table 25 - List of get/set commands....97
Table 26 - List of basic SMS diagnostics RDB variables 97
Table 27 - SMS diagnostics example commands....99
Table 28 - System log detail levels 101
Table 29 - Administration configuration options....109
Table 24 - LAN Management Default Settings....120
Table 25 - Web Interface Default Settings 120
Table 26 - Telnet Access 120
Table 27 - RJ-45 connector pin outs....127
Table 34 - RS-232 Wiring 128
Table 35 - RS-485 Half Duplex Wiring....128
Table 36 - RS-485 (RS-422) Full Duplex Wiring 128
Table 39 - Technical Specifications of the NWL-15 router....134

Appendix B: Device mounting dimensions

The image below is at 100% scale and may be used as a template for mounting the device. All dimensions shown are in millimeters.

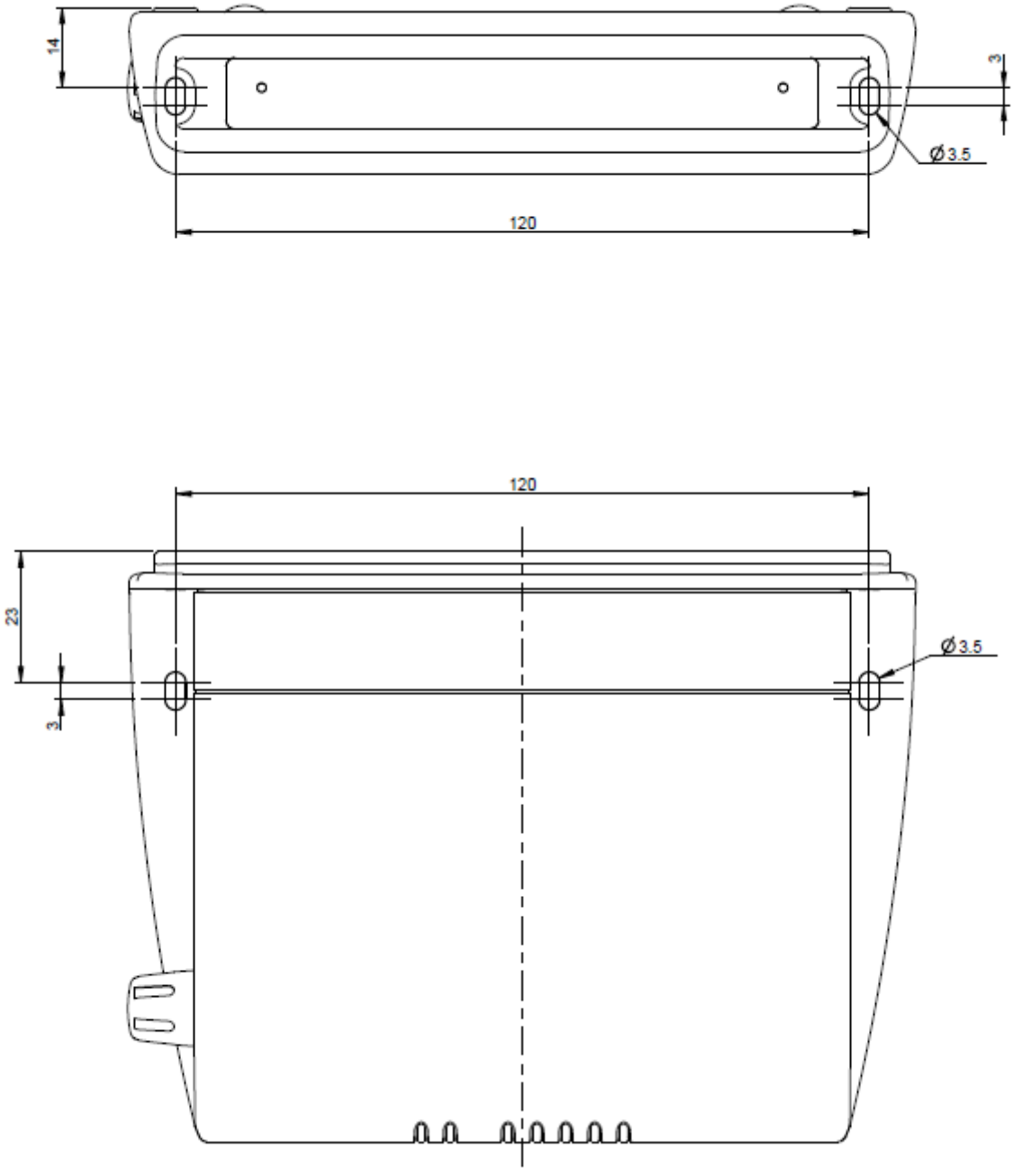


Figure 123 - Device mounting dimensions

Appendix C: Mounting bracket

The image below is at 100% scale and may be used as a template for mounting the bracket. All dimensions shown are in millimeters.

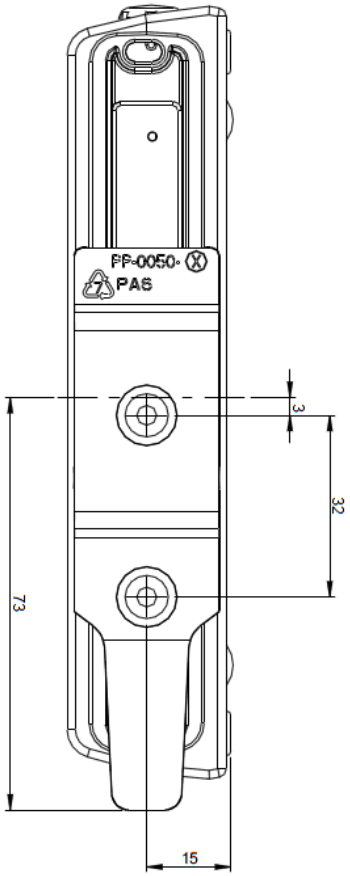


Figure 124 - Mounting bracket

Appendix D: Default settings

The following tables list the default settings for the NWL-15 router.

LAN (MANAGEMENT)	
Static IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1

Table 30 - LAN Management Default Settings

ADMIN MANAGER ACCOUNT		ROOT MANAGER ACCOUNT	
Username:	admin	Username:	root
Password:	admin	Password:	admin

Table 31 - Web Interface Default Settings

Note: The admin manager account allows you to manage all settings of the router except functions such as firmware upgrade, device configuration backup and restore and reset to factory default settings, which are privileged only to the root manager account.

NWL-15 ROUTER TELNET ACCESS	
Username:	root
Password:	admin

Table 32 - Telnet Access

Restoring factory default settings

Restoring factory defaults will reset the NWL-15 router to its factory default configuration. You may encounter a situation where you need to restore the factory defaults on your NWL-15 router such as:

- You have lost your username and password and are unable to login to the web configuration page;
- You are asked to perform a factory reset by support staff.

There are two methods you can use to restore factory default settings on your NWL-15 router:

- Using the web-based user interface
- Using the reset button on the interface panel of the router

Using the web-based user interface

To restore your router to its factory default settings, please follow these steps:

1. Open a browser window and navigate to the IP address of the router (default address is http://192.168.1.1). Login to the router using **root** as the User Name and **admin** as the password.
2. Click the **System** item from the top menu bar, then **System Configuration** on the left menu and then click **Settings Backup / Restore**.
3. Under the **Restore factory defaults** section, click the **Restore Defaults** button. The router asks you to confirm that you wish to restore factory defaults. Click **OK** to continue. The router sets all settings to default. Click **OK** again to reboot the router.
4. When the Power light returns to a steady red, the reset is complete. The default settings are now restored.

Using the reset button on the interface panel of the router

Use a pen to depress the Reset button on the device for 15-20 seconds. The router will restore the factory default settings and reboot.

When you have reset your NWL-15 router to its default settings you will be able to access the device's configuration web interface using http://192.168.1.1 with username **admin** or **root** and password **admin**.

Appendix E: Recovery mode

The NWL-15 router features two independent operating systems, each with its own file systems. These two systems are referred to as 'Main' and 'Recovery'. It is always possible to use one in order to restore the other in the event that one system becomes damaged or corrupted (such as during a firmware upgrade failure). The recovery console provides limited functionality and is typically used to restore the main firmware image in the case of a problem.

Accessing recovery mode

Both systems have web interfaces that can be used to manipulate the other inactive system. The NWL-15 router starts up by default in the Main system mode, however the router may be triggered to start in recovery mode if desired.

To start the router in recovery mode:

1. Press and hold the physical reset button on the interface panel of the router for 5 to 15 seconds. When the LEDs on the front panel change to amber and countdown in a sequence, release the reset button. The router then boots into recovery mode.
2. In your browser, navigate to http://192.168.1.1. The router's recovery mode is hardcoded to use this address regardless of the IP address that was configured in the main system. The router's recovery console is displayed.

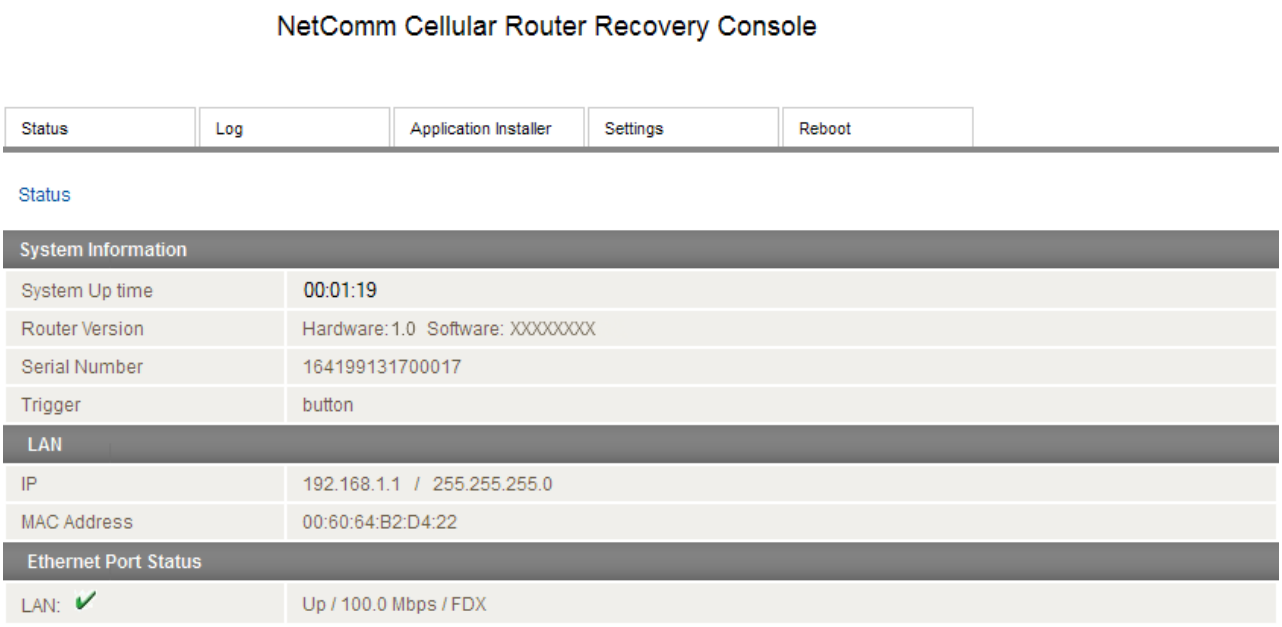


Figure 125 - Recovery console

Status

The status page provides basic information such as the system up time, hardware and software router versions, the router's serial number, the method used to trigger the recovery mode, the IP and MAC address of the router and the status of the Ethernet port.

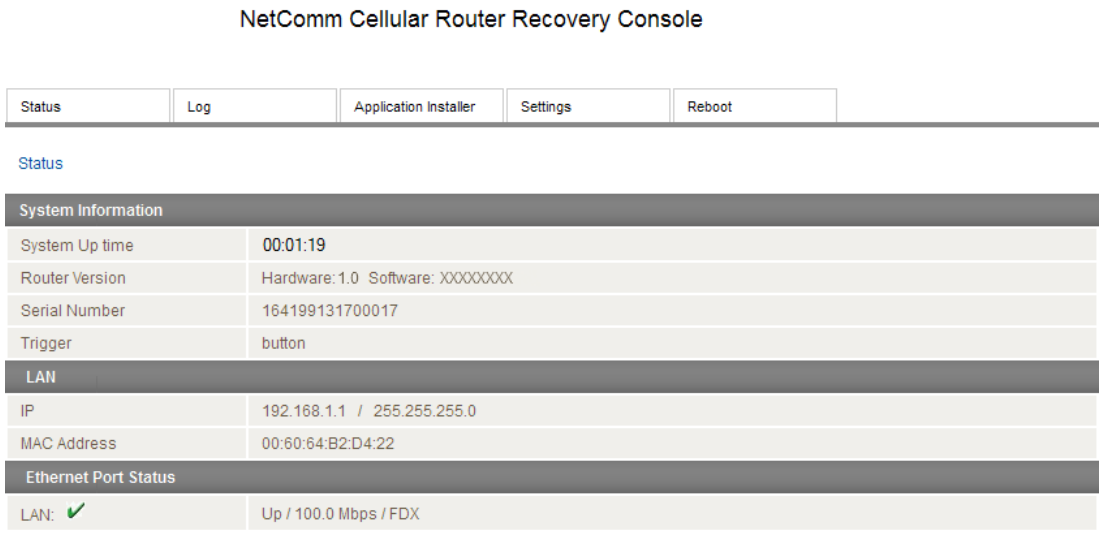
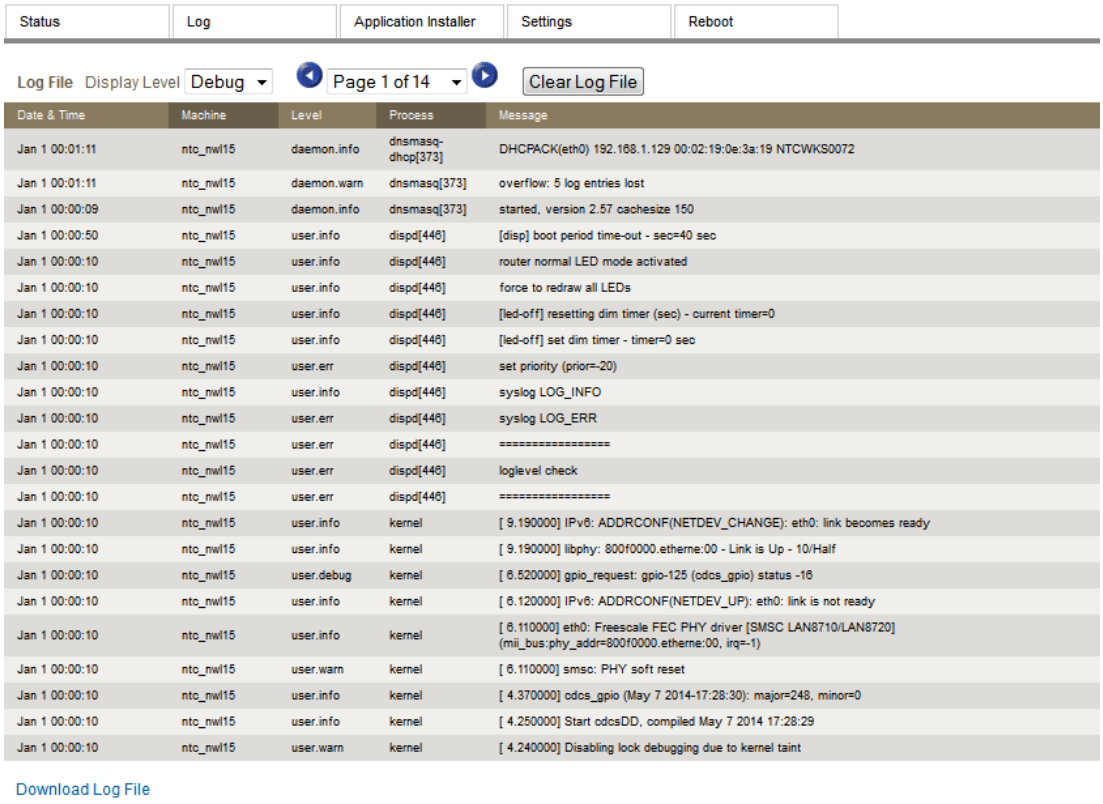


Figure 126 - Recovery mode - Status

Log

The log page displays the system log which is useful in troubleshooting problems which may have led to the router booting up in recovery mode. The only functionality provided here is the ability to clear the system log, filter by log level and downloading of the log file.



Date & Time	Machine	Level	Process	Message
Jan 1 00:01:11	ntc_nwl15	daemon.info	dnsmasq-dhcp[373]	DHCPACK(eth0) 192.168.1.129 00:02:19:0e:3a:19 NTCWKS0072
Jan 1 00:01:11	ntc_nwl15	daemon.warn	dnsmasq[373]	overflow: 5 log entries lost
Jan 1 00:00:09	ntc_nwl15	daemon.info	dnsmasq[373]	started, version 2.57 cachesize 150
Jan 1 00:00:50	ntc_nwl15	user.info	dispd[446]	[disp] boot period time-out - sec=40 sec
Jan 1 00:00:10	ntc_nwl15	user.info	dispd[446]	router normal LED mode activated
Jan 1 00:00:10	ntc_nwl15	user.info	dispd[446]	force to redraw all LEDs
Jan 1 00:00:10	ntc_nwl15	user.info	dispd[446]	[led-off] resetting dim timer (sec) - current timer=0
Jan 1 00:00:10	ntc_nwl15	user.info	dispd[446]	[led-off] set dim timer - timer=0 sec
Jan 1 00:00:10	ntc_nwl15	user.err	dispd[446]	set priority (prior=-20)
Jan 1 00:00:10	ntc_nwl15	user.info	dispd[446]	syslog LOG_INFO
Jan 1 00:00:10	ntc_nwl15	user.err	dispd[446]	syslog LOG_ERR
Jan 1 00:00:10	ntc_nwl15	user.err	dispd[446]	=================
Jan 1 00:00:10	ntc_nwl15	user.err	dispd[446]	loglevel check
Jan 1 00:00:10	ntc_nwl15	user.err	dispd[446]	=================
Jan 1 00:00:10	ntc_nwl15	user.info	kernel	[9.190000] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Jan 1 00:00:10	ntc_nwl15	user.info	kernel	[9.190000] libphy: 800f0000.etherne:00 - Link is Up - 10/Half
Jan 1 00:00:10	ntc_nwl15	user.debug	kernel	[6.520000] gpio_request: gpio-125 (cdcs_gpio) status -16
Jan 1 00:00:10	ntc_nwl15	user.info	kernel	[6.120000] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
Jan 1 00:00:10	ntc_nwl15	user.info	kernel	[6.110000] eth0: Freescale FEC PHY driver [SMSC LAN8710/LAN8720] (mii_bus:phy_addr=800f0000.etherne:00, irq=-1)
Jan 1 00:00:10	ntc_nwl15	user.warn	kernel	[6.110000] smsc: PHY soft reset
Jan 1 00:00:10	ntc_nwl15	user.info	kernel	[4.370000] cdcs_gpio (May 7 2014-17:28:30): major=248, minor=0
Jan 1 00:00:10	ntc_nwl15	user.info	kernel	[4.250000] Start cdcsDD, compiled May 7 2014 17:28:29
Jan 1 00:00:10	ntc_nwl15	user.warn	kernel	[4.240000] Disabling lock debugging due to kernel taint

Figure 127 - Recovery mode – Log

Application installer

The Application installer is designed to upload and install main firmware images, upload recovery firmware images, custom applications and HTTPS certificates. Use the **Browse** button to select a file to be uploaded to the router. When it has been selected, press the **Upload** button. The file is sent to the router and when the transfer is complete, the file appears in the Uploaded files list. From the Uploaded files list, you are able to either **Install** or **Delete** a file.

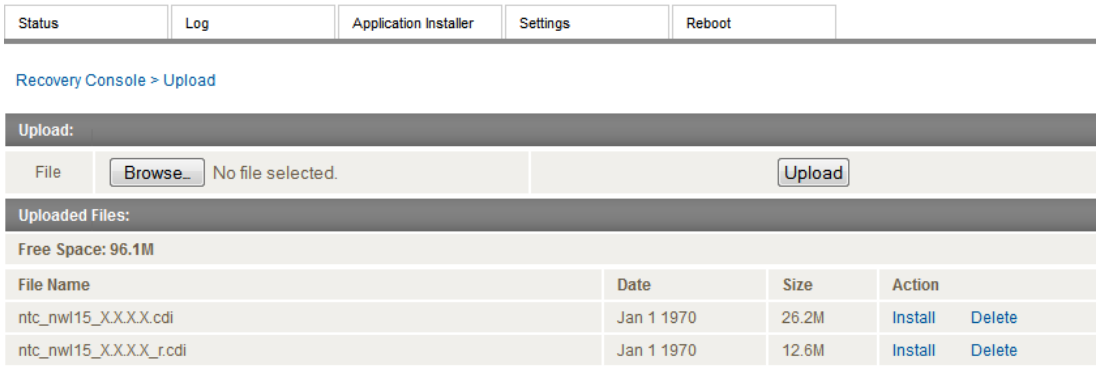


Figure 128 - Recovery mode - Application Installer

Settings

The settings page provides the option of restoring the router to factory default settings. Click the **Restore** button to set the router back to the original factory settings.

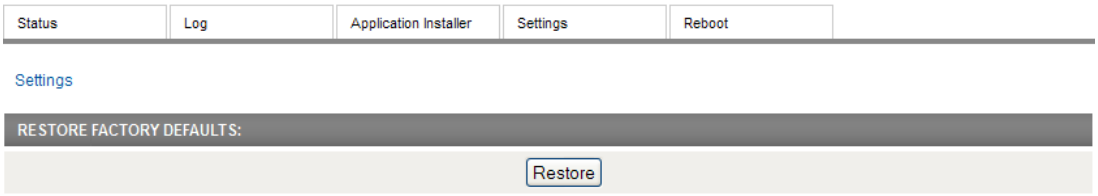


Figure 129 - Recovery mode – Settings

Reboot

The reboot page allows you to reboot the router when you have finished using recovery mode. When rebooting the router from recovery mode, the router boots into the main firmware image unless there is some fault preventing it from doing so, in which case the recovery console will be loaded.

Click the **Reboot** button to reboot the router to the main firmware image.

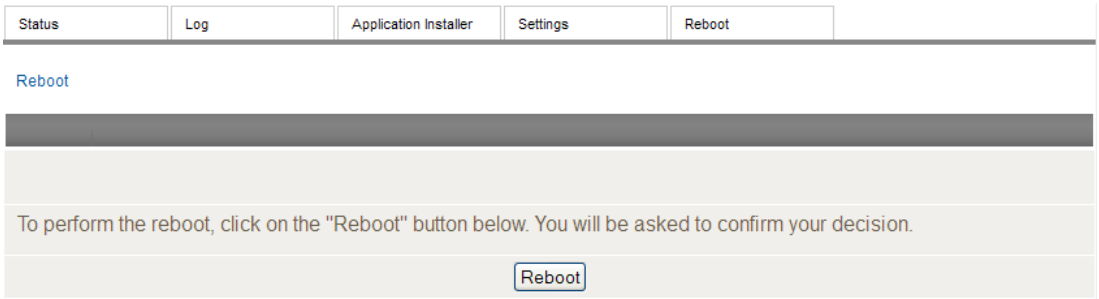


Figure 130 - Recovery mode - Reboot

Appendix F: HTTPS - Uploading a self-signed certificate

If you have your own self-signed certificate or one purchased elsewhere and signed by a Certificate Authority, you can upload it to the NWL-15 router using the Upload page.

Note: Your key and certificate files must be named **server.key** and **server.crt** respectively otherwise they will not work.

To upload your certificate:

1. Click on the **System** item from the top menu bar. From the side menu bar, select **System Configuration** and then **Upload**. The file upload screen is displayed.

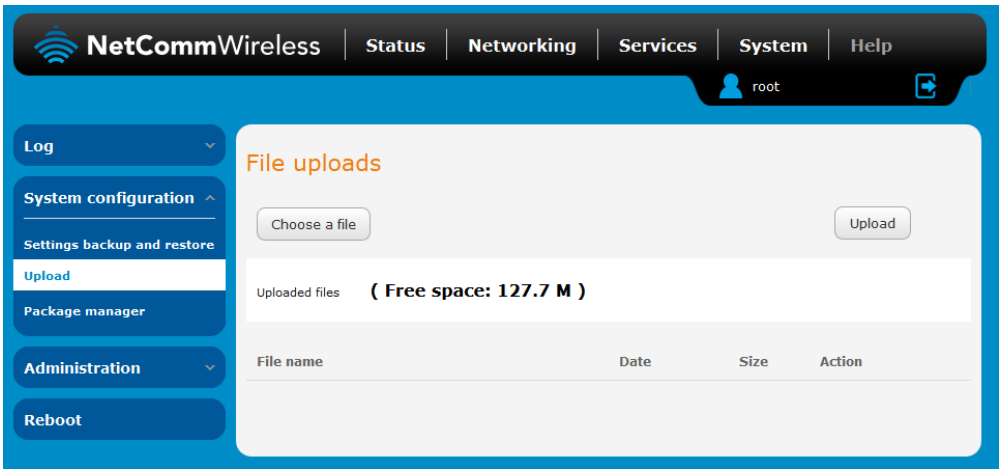


Figure 131 - Upload page

2. Click the **Choose a File** button and locate your server certificate file and click **Open**.

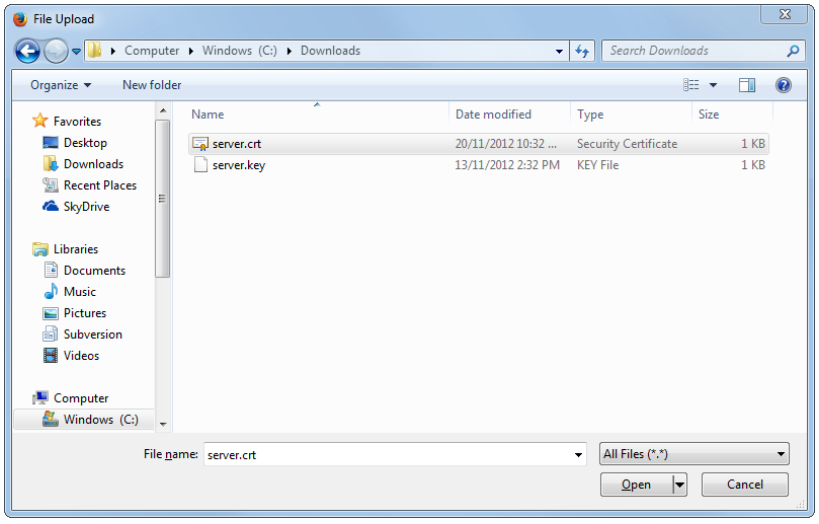


Figure 132 - Browse for server.crt

3. Click the **Upload** button to begin uploading it to the router. The file appears in the list of files stored on the router.

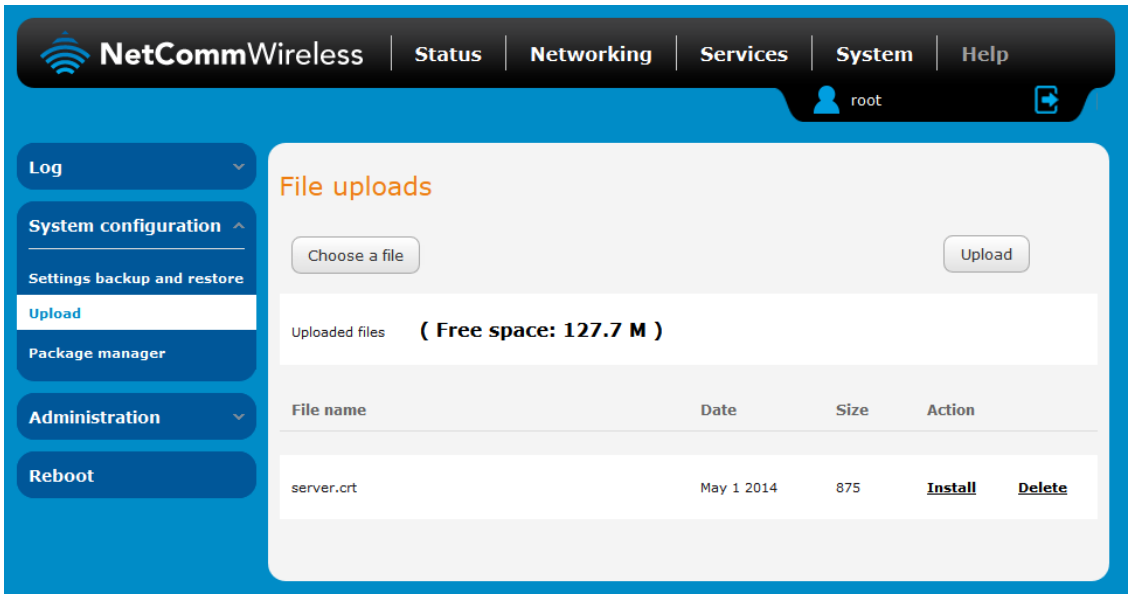


Figure 133 - Server certificate file uploaded

4. Repeat steps 2 and 3 for the server key file.
5. Click the **Install** link next to the server.crt file then click **OK** on the prompt that is displayed. The certificate file is installed. Repeat this for the key file. When each file is installed it is removed from the list of stored files.

Figure 134 - Installing the server.crt file

Appendix G: RJ-45 connector

The RJ-45 connector provides an interface for a data connection and for device input power using the pin layout shown below.

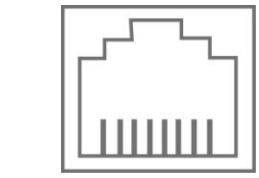


Figure 135 -The RJ-45 connector

PIN	COLOUR	SIGNAL (802.3AF MODE A)	SIGNAL (802.3AF MODE B)
1	White/Orange stripe	Rx +	Rx + DC +
2	Orange Solid	Rx -	Rx - DC +
3	White/Green stripe	Tx +	Tx + DC -
4	Blue solid	DC +	unused
5	White/Blue stripe	DC +	unused
6	Green solid	Tx -	Tx - DC -
7	White/Brown stripe	DC -	unused
8	Brown solid	DC -	unused

Table 33 - RJ-45 connector pin outs

Appendix H: Serial port wiring

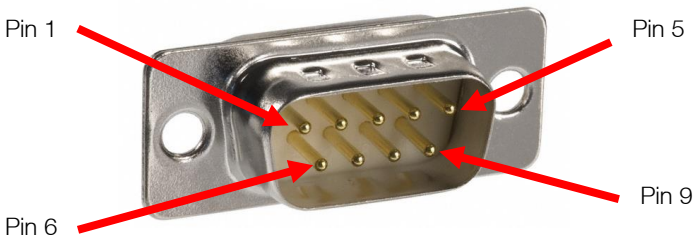


Figure 136 - DE9 Male connector (Pin side view)

The NWL-15 router has a serial interface and acts as the data communications equipment (DCE). The wiring tables below indicate the DCE and DTE devices as well as the signal direction. Shielding cable can optionally be soldered to the chassis and connected to ground.

DTE DEVICE (COMPUTER)			SIGNAL DIRECTION	DCE DEVICE (NWL-15 ROUTER)		
PIN	NAME	DESCRIPTION		DESCRIPTION	NAME	PIN
1	DCD	Data carrier detect	←	Data carrier detect	DCD	1
2	RXD	Receive Data	←	Receive Data	RXD	2
3	TXD	Transmit Data	→	Transmit Data	TXD	3
4	DTR	Data Terminal Ready	→	Data Terminal Ready	DTR	4
5	GND	Ground	—	Ground	GND	5
6	DSR	Data Set Ready	←	Data Set Ready	DSR	6
7	RTS	Request to Send	→	Request to Send	RTS	7
8	CTS	Clear to Send	←	Clear to Send	CTS	8
9	RI	Ring Indicator	←	Ring Indicator	RI	9
-	FGND	Shield (Soldered to D9 metal shield)	—	Shield (Soldered to D9 metal shield)	FGND	-

Table 34 - RS-232 Wiring

RS-485 HALF DUPLEX WIRING			
PIN	SIGNAL	NAME	DESCRIPTION
1	—	A	Differential pair A
2	+	B	Differential pair B
5		GND	Ground

Table 35 - RS-485 Half Duplex Wiring

RS-485 (RS-422) FULL DUPLEX WIRING			
PIN	SIGNAL	NAME	DESCRIPTION
1	—	RXA	Receive (Differential pair A)
2	+	RXB	Receive (Differential pair B)
3	+	TXB	Transmit (Differential pair B)
4	—	TXA	Transmit (Differential pair A)
5		GND	Ground

Table 36 - RS-485 (RS-422) Full Duplex Wiring

Appendix I: Inputs/Outputs

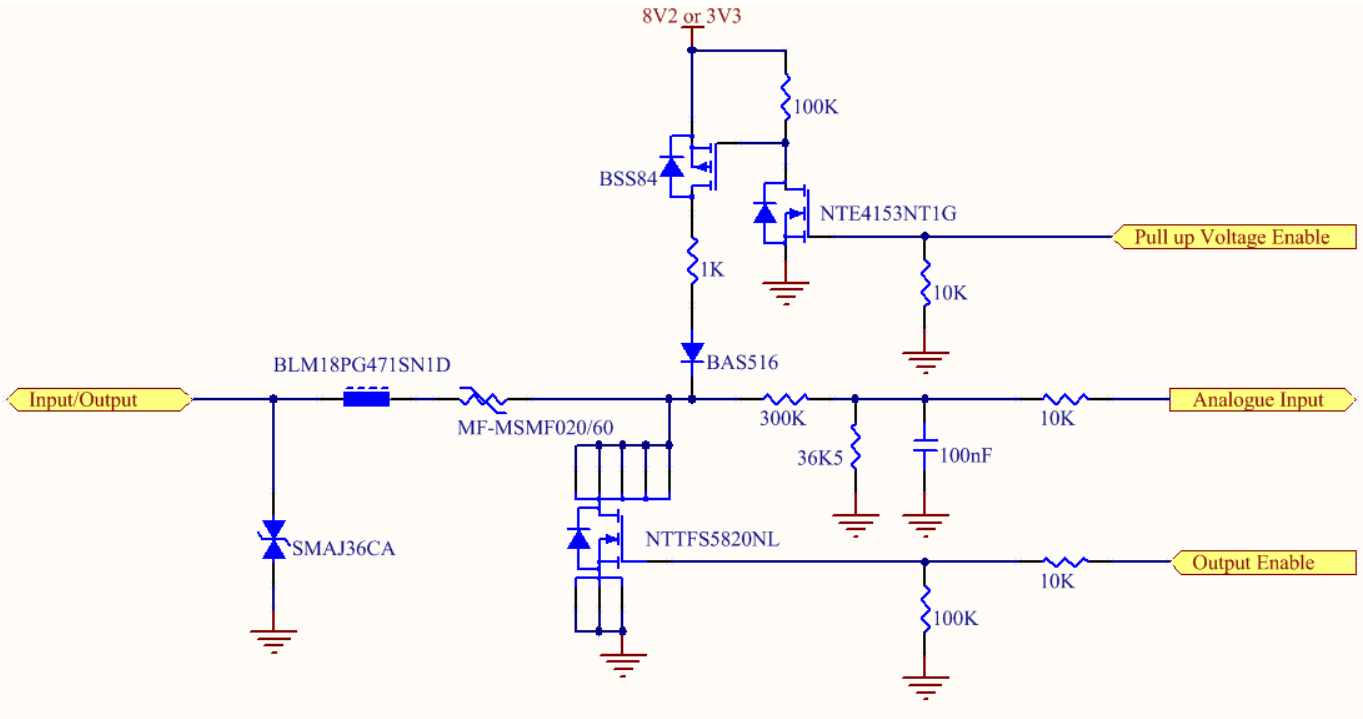
Overview

The NWL-15 router is equipped with a 6-way terminal block connector providing 3 identical multipurpose inputs and outputs as well as a dedicated ignition input. These inputs and outputs may be independently configured for various functions, including:

- NAMUR (EN 60947-5-6 / IEC 60947-5-6) compatible sensor input
- Proximity sensor input for use with contact closure (open/closed) type of sensors (PIR sensors, door/window sensors for security applications) with the input tamper detection possible (four states detected: open, closed, short and break) by the use of external resistors
- Analogue 0V to 30V input
- Digital input (the I/O voltage measured by the Analogue input and the software making a decision about the input state) with the threshold levels configurable in software
- Open collector output.

Hardware interface

The interface of the 3 multipurpose inputs/outputs are based on the circuit diagram below



The **Input/Output** label is the physical connection to the outside world. There are protection devices and resistor dividers to condition the signal prior to it going into the processor. The three labels to the right are the interface to the processor. **Output Enable** activates the Transistor which provides an open collector (ground) output and can sink 200mA at 23°C. It is protected by a resettable fuse and transient protection diode. If used with the pull up resistor, which can be activated by the **Pull up Voltage Enable** pin, then you can have a High or Low output rather than open drain. The resistor can be pulled up to 3V3 for Cmos compatible output or 8.2V by software. The **Analogue Input** pin can read values from 0V to 30V. It is divided by a resistor network to read appropriate levels in the processor. Depending on the sensor type used, the pull up resistor can be switched on or off. If using the NAMUR sensor configuration the pull up will be activated to 8V2 by default.

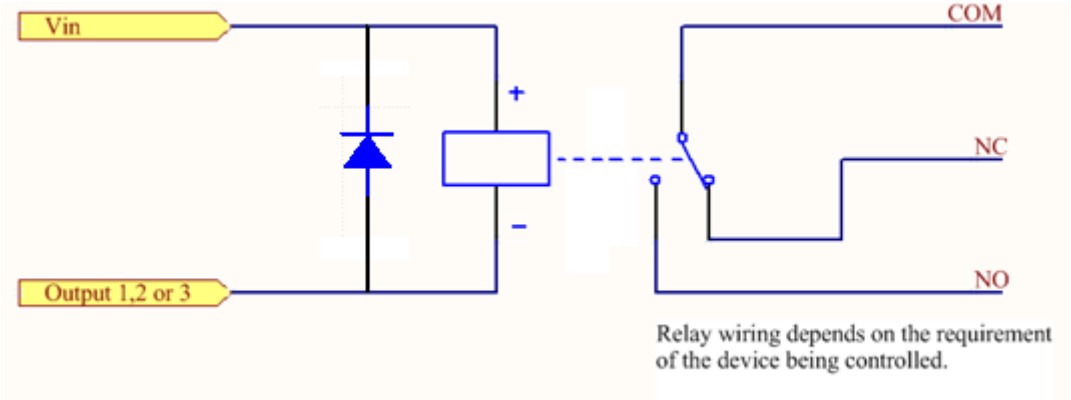
Wiring examples

The following examples are shown as a guide as to what can be achieved by the I/O features. It is up to the system integrator to have enough knowledge about the interface to be able to achieve the required results.

Note: NetComm Wireless does not offer any further advice on the external wiring requirements or wiring to particular sensors, and will not be responsible for any damage to the unit or any other device used in conjunction with it. Using outputs to control high voltage equipment can be dangerous. The integrator must be a qualified electrician if dealing with mains voltages controlled by this unit.

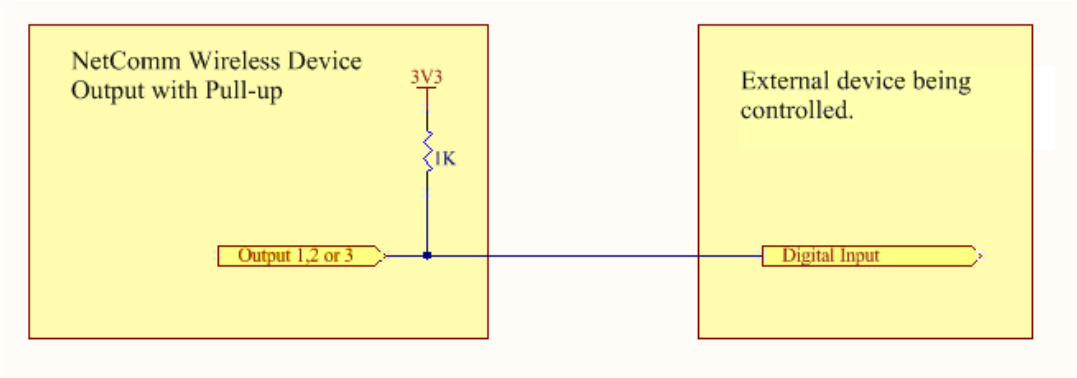
Open collector output driving a relay

Any output can be configured to control a relay. This is an example where the transistor will supply the ground terminal of the solenoid. External voltage is supplied to the other side of the solenoid.



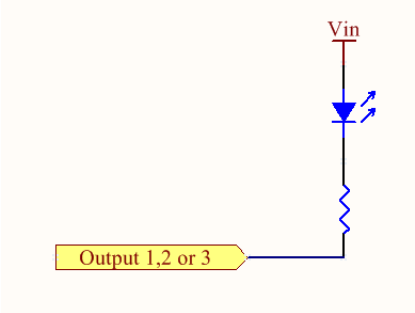
Logic level output

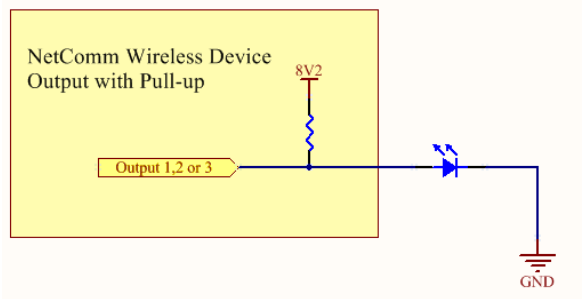
An output can be used with the pull up resistor to provide a logic level output which would be suitable to control an external digital device.



LED output

An LED can be controlled by simply providing an open collector ground to an externally powered LED Resistor value and Voltage will need to suit the LED type used. Alternatively an LED can be powered using 8V2 via 1K resistor. The suitability of the LED will need to be investigated.

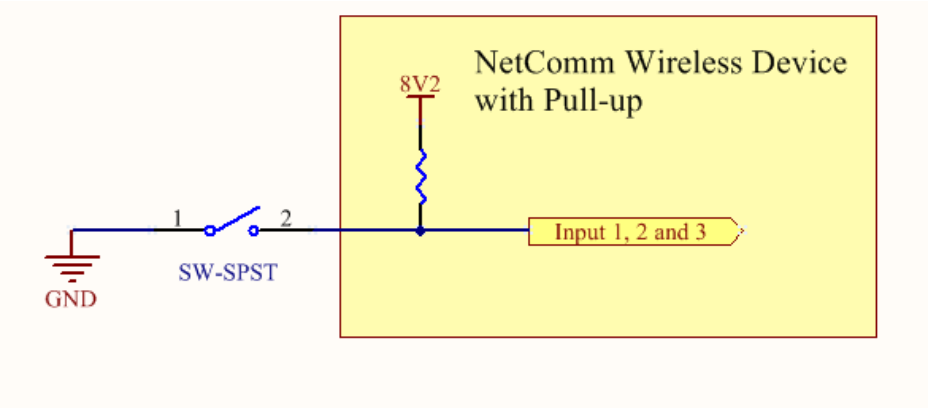




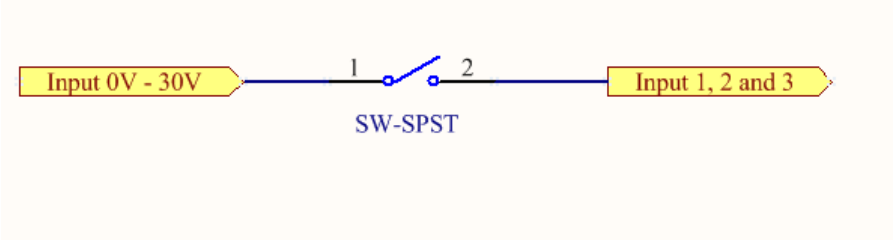
Digital inputs

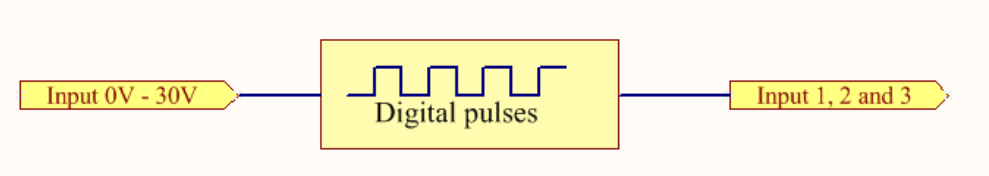
There are several ways to connect a digital input. A digital input can be anything from a simple switch to a digital waveform or pulses. The unit will read the voltage in as an analogue input and the software will decode it in a certain way depending on your configuration.

Below is a contact closure type input, which is detecting an Earth. Pull up is activated for this to work.



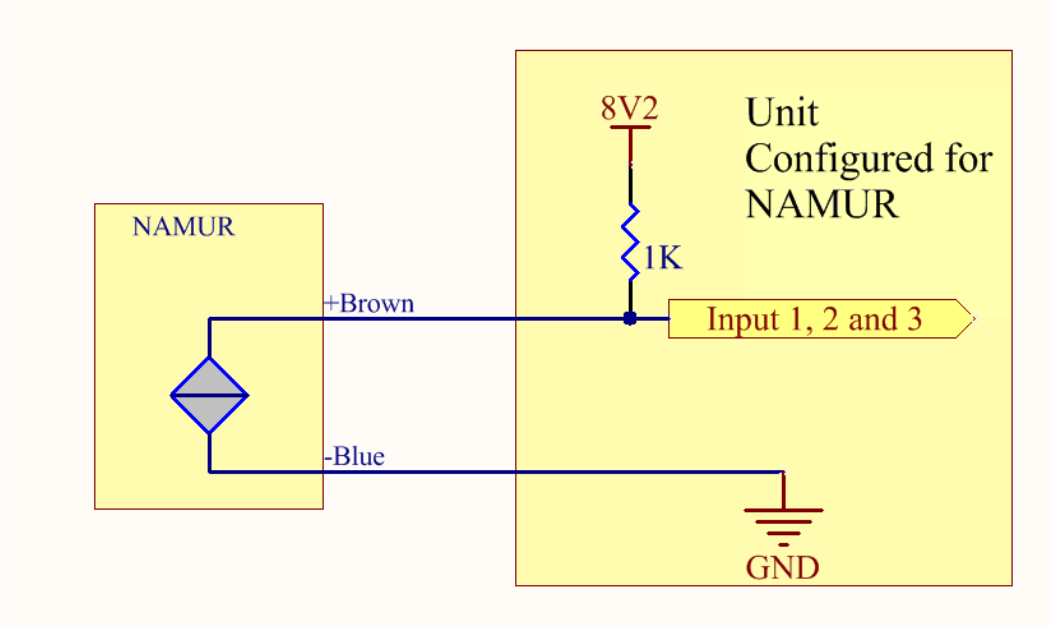
The following input detects an input going high. The turn on/off threshold can be set in the software.





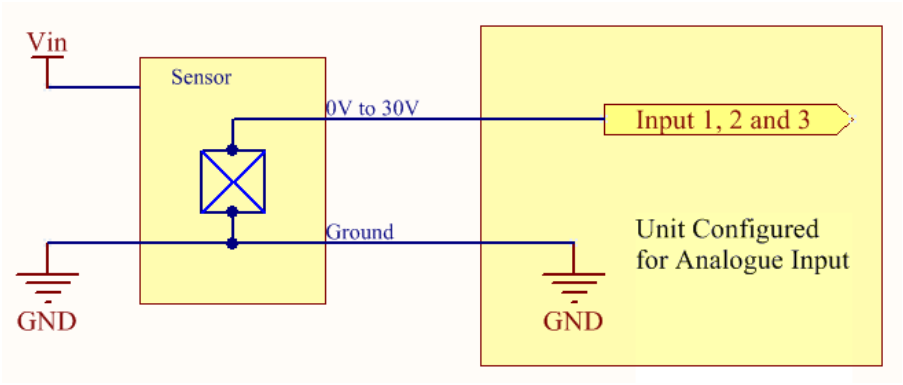
NAMUR sensor

A NAMUR sensor is a range of sensors which conform to the EN 60947-5-6 / IEC 60947-5-6 standards. They basically have two states which are reflected by the amount of current running through a sense resistor.



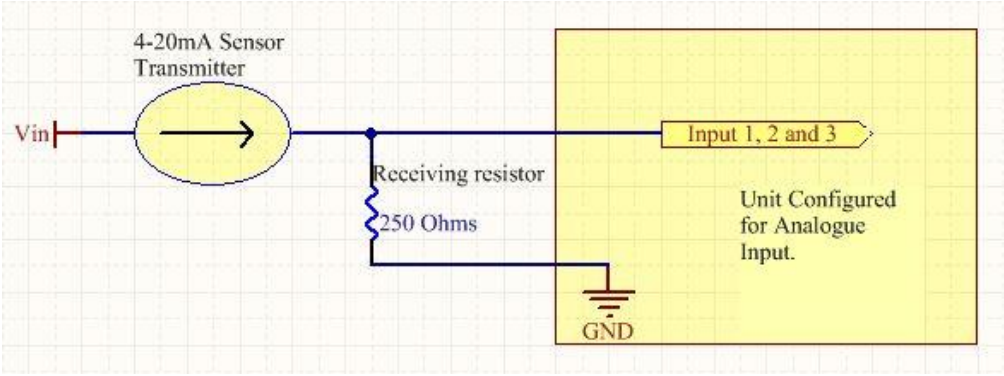
Analogue sensor with voltage output

There are various analogue sensors that connect directly to the unit which can provide a voltage output. These would require an external power source which may or may not be the same as the unit itself. The voltage range they provide can be between 0V and 30V. Some common sensor output ranges include 0V to 10V. These would work on the unit, The pull up resistor is not activated in this case.



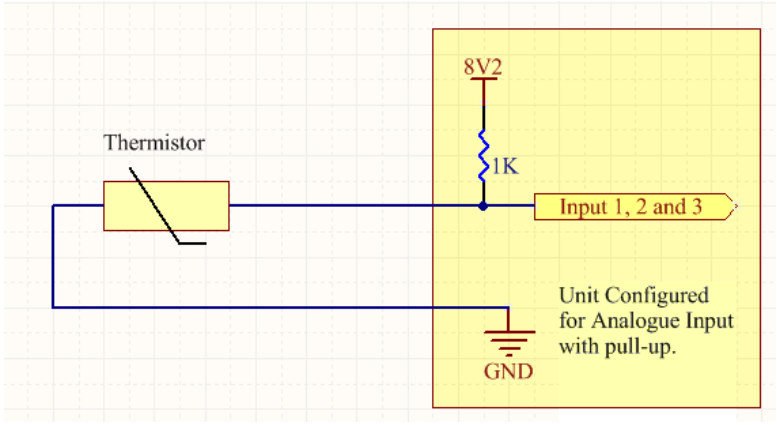
Analogue sensor with 4 to 20mA output

Another common type of sensor type is the 4-20mA current loop sensor. It provides a known current through a fixed resistor, usually 250 ohms thus producing a voltage of 0v to 5V at the input. The sensor would require an external power source which may or may not be the same as the unit itself. It will also require an external resistor. The internal pull up resistor is not activated.



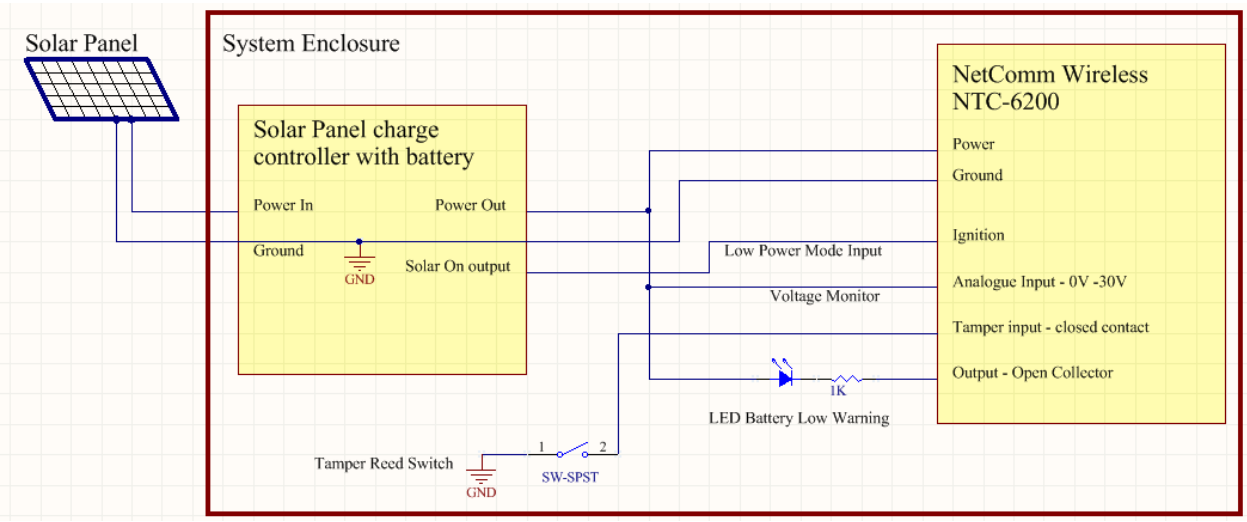
Analogue sensor with thermistor

Some sensors work by changing resistance due to a change, such as temperature, light etc. These may be wired up to an external or internal power source and the resistance can be read into the analogue signal. This will require some software calibration like scaling or offset to map the voltage received to the sensor resistor value. An example below shows the internal pull-up voltage and 1K resistor activated. The voltage received depends on the combination of resistors and the value of the resistance of the sensor itself.



System example –Solar powered router with battery backup

The previous examples of wiring can be used to come up with a system. The following test case is an example of how the I/O's can be used to enhance a simple router setup.



Technical data

The following table lists the hardware specifications of the NWL-15.

COMPONENT	SPECIFICATION
Memory	256MByte Flash memory storage (~120MB available on board space for user storage)
Operating System	Embedded Linux 3.6
Cellular bands	CDMA (BC0/BC1), 800/1900MHz
Maximum Data Throughput / 3G Radio interface	EV-DO Rev.A data rates: FL max. 3.1Mbps, RL max. 1.8Mbps 1xRTT Advanced data rates: FL max. 307.2kbps, RL max. 307.2kbps
Connectivity	1x (RJ-45) 10/100Base-TX Port with Auto MDIX 1x RS232 Serial Port DB-9 female DCE supporting either 9 wire RS232 or RS422 (software selectable) Software controlled termination resistors for RS485 Mini USB 2.0 OTG interface with 0.5A supply capability 3 x Multipurpose I/O pins
Antenna connectors	2x SMA connectors for cellular (1x Main and 1x RX Diversity) 1x SMA connector for GPS
LED Indicators	7x tri-colour LEDs. Power, Network and 5x Signal Strength indicators
GPS	Embedded GPS receiver (1575.42Mhz) Active antenna voltage: 3.05V Maximum current: 50mA Tracking sensitivity under open sky: -159dBm Acquisition sensitivity under open sky: -149dBm Cold start sensitivity: -145dBm Time to first fix (TTFF): Cold 25s, Warm 10s, Hot 3s Short circuit protection Supports NMEA-0183 (v2.3) Redirect NMEA stream to serial for forward over IP Odometer reading available via Web-UI, CLI and SDK
Operating Temperature	Operating Temperature Range: -20°C ~ +65°C Storage Temperature Range: -30°C ~ +80°C
Power input	Power input and I/O's via 6 way termination block receptacle Field terminable power input via screw type terminal block included DC Power (8 - 40V DC) Vehicle compatible protection on DC Input Jack. (ISO7637 standard) Recommended power input rating of 6W via DC terminal block (e.g 12V 1.5A)
Dimensions & Weight	135mm (L) x 101mm (W) x 29mm (D) / 180g
Regulatory Compliance	FCC

Table 37 - Technical Specifications of the NWL-15 router

Safety and product care

RF exposure

Your device contains a transmitter and a receiver. When it is on, it receives and transmits RF energy. When you communicate with your device, the system handling your connection controls the power level at which your device transmits.

This device meets the government's requirements for exposure to radio waves.

This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. To ensure compliance with RF exposure guidelines the device must be used with a minimum of 20cm separation from the body. Failure to observe these instructions could result in your RF exposure exceeding the relevant guideline limits.

External antenna

Any optional external antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operated in conjunction with any other antenna or transmitter. Please consult the health and safety guide of the chosen antenna for specific body separation guidelines as a greater distance of separation may be required for high-gain antennas.

Any external antenna gain must meet RF exposure and maximum radiated output power limits of the applicable rule section. The maximum antenna gain for this device as reported to the FCC is: 9.4 dBi (850MHz) and 8.4 dBi (1900MHz).

FCC statement

FCC compliance

Federal Communications Commission Notice (United States): Before a wireless device model is available for sale to the public, it must be tested and certified to the FCC that it does not exceed the limit established by the government-adopted requirement for safe exposure.

FCC regulations

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorientate or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.

Electrical safety

Accessories

Only use approved accessories.

Do not connect with incompatible products or accessories.

Connection to a car

Seek professional advice when connecting a device interface to the vehicle electrical system.

Distraction

Operating machinery

Full attention must be given to operating the machinery in order to reduce the risk of an accident.

Product handling

You alone are responsible for how you use your device and any consequences of its use.

You must always switch off your device wherever the use of a mobile phone is prohibited. Do not use the device without the clip-on covers attached, and do not remove or change the covers while using the device. Use of your device is subject to safety measures designed to protect users and their environment.

Always treat your device and its accessories with care and keep it in a clean and dust-free place.

Do not expose your device or its accessories to open flames or lit tobacco products.

Do not expose your device or its accessories to liquid, moisture or high humidity.

Do not drop, throw or try to bend your device or its accessories.

Do not use harsh chemicals, cleaning solvents, or aerosols to clean the device or its accessories.

Do not paint your device or its accessories.

Do not attempt to disassemble your device or its accessories, only authorised personnel must do so.

Do not use or install this product in extremely hot or cold areas. Ensure that the device is installed in an area where the temperature is within the supported operating temperature range (-20°C to 65°C)

Do not use your device in an enclosed environment or where heat dissipation is poor. Prolonged use in such space may cause excessive heat and raise ambient temperature, which will lead to automatic shutdown of your device or the disconnection of the mobile network connection for your safety. To use your device normally again after such shutdown, cool it in a well-ventilated place before turning it on.

Please check local regulations for disposal of electronic products.

Do not operate the device where ventilation is restricted

Installation and configuration should be performed by trained personnel only.

Do not use or install this product near water to avoid fire or shock hazard. Avoid exposing the equipment to rain or damp areas.

Arrange power and Ethernet cables in a manner such that they are not likely to be stepped on or have items placed on them.

Ensure that the voltage and rated current of the power source match the requirements of the device. Do not connect the device to an inappropriate power source.

Small children

Do not leave your device and its accessories within the reach of small children or allow them to play with it.

They could hurt themselves or others, or could accidentally damage the device.

Your device contains small parts with sharp edges that may cause an injury or which could become detached and create a choking hazard.

Emergency & other situations requiring continuous connectivity

This device, like any wireless device, operates using radio signals, which cannot guarantee connection in all conditions. Therefore, you must never rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss.

Device heating

Your device may become warm during normal use.

Faulty and damaged products

Do not attempt to disassemble the device or its accessories.

Only qualified personnel must service or repair the device or its accessories.

If your device or its accessories have been submerged in water punctured or subjected to a severe fall, do not use until they have been checked at an authorised service centre.

Interference

Care must be taken when using the device in close proximity to personal medical devices, such as pacemakers and hearing aids.

Pacemakers

Pacemaker manufacturers recommend that a minimum separation of 15cm be maintained between a device and a pacemaker to avoid potential interference with the pacemaker.

Hearing aids

People with hearing aids or other cochlear implants may experience interfering noises when using wireless devices or when one is nearby.

The level of interference will depend on the type of hearing device and the distance from the interference source, increasing the separation between them may reduce the interference. You may also consult your hearing aid manufacturer to discuss alternatives.

Medical devices

Please consult your doctor and the device manufacturer to determine if operation of your device may interfere with the operation of your medical device.

Hospitals

Switch off your wireless device when requested to do so in hospitals, clinics or health care facilities. These requests are designed to prevent possible interference with sensitive medical equipment.

Interference in cars

Please note that because of possible interference to electronic equipment, some vehicle manufacturers forbid the use of devices in their vehicles unless an external antenna is included in the installation.

Explosive environments

Petrol stations and explosive atmospheres

In locations with potentially explosive atmospheres, obey all posted signs to turn off wireless devices such as your device or other radio equipment.

Areas with potentially explosive atmospheres include fuelling areas, below decks on boats, fuel or chemical transfer or storage facilities, areas where the air contains chemicals or particles, such as grain, dust, or metal powders.

Blasting caps and areas

Turn off your device or wireless device when in a blasting area or in areas posted turn off “two-way radios” or “electronic devices” to avoid interfering with blasting operations.

Product warranty

For warranty information please visit http://www.netcommwireless.com/product/m2m/nwl-15